**Міністерство освіти і науки України**

**Національний технічний університет**

**«Дніпровська політехніка»**

---

**Інститут електроенергетики**

**Факультет інформаційних технологій**

**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи ступеню бакалавра

**студентки** ***Таран Катерини Сергіївни***

**академічної групи** ***УБіт-15-1***

**напряму підготовки** ***6.170103 Управління інформаційною безпекою***

**спеціалізації**[1]

**за освітньо-професійною програмою**

**на тему** ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ПП «ТехноСервіс»***

| **Керівники** | **Прізвище, ініціали** | **Оцінка за шкалою** | | **Підпис** |
|---|---|---|---|---|
| | | **рейтинговою** | **інституційною** | |
| кваліфікаційної роботи | д.ф.-м.н.,проф.Кагадій Т.С. | | | |
| розділів: | | | | |
| спеціальний | ст.в. Тимофєєв Д.С. | | | |
| економічний | к.е.н., доц. Пілова Д.П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**

**2019**

**ЗАТВЕРДЖЕНО:**

завідувач кафедри

безпеки інформації та телекомунікацій

_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ

## на кваліфікаційну роботу

## ступеня бакалавра

**студентки** ***Таран Катерини Сергіївни*** **академічної групи** ***УБіт-15-1***

(прізвище ім'я по-батькові) (шифр)

**напряму підготовки** *6.170103 Управління інформаційною безпекою*

(код і назва спеціальності)

**на тему** ***Розробка політики безпеки інформації інформаційно-телекомунікайної системи ПП «ТехноСервіс»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2019 № 771-л

| Розділ | Зміст | Термін виконання |
|---|---|---|
| Розділ 1 | Аналіз нормативно-правової бази в сфері захисту інформації, актуальність проблеми захисту інформації в ІТС, задачі на розробку КСЗІ на ОІД. | 20.03.2019 |
| Розділ 2 | Обстеження на об'єкті інформаційної діяльності, аналіз середовища функціонування, аналіз ризиків, основні положення політики безпеки інформації. | 30.05.2019 |
| Розділ 3 | Економічна доцільність впровадження політики безпеки, розрахунки витрат та ефекту від впровадження КСЗІ. | 15.06.2019 |

**Завдання видано** _____ Кагадій Т.С.

(підпис керівника) (прізвище, ініціали)

**Дата видачі: 08.01.2019р.**

**Дата подання до екзаменаційної комісії: 17.06.2019р.**

**Прийнято до виконання** _____ Таран К.С.

(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: с., рис., табл., додатків, джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система (ІТС) ПП «ТехноСервіс».

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності (ОІД).

Мета роботи (проекту): розробити політику безпеки інформації (ПБ) в ІТС ПП «ТехноСервіс».

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі проведено аналіз нормативно-правової бази у сфері захисту інформації та визначена актуальність проблеми захисту інформації в ІТС комерційних підприємств, встановлені задачі на розробку комплексної системи захисту інформації КСЗІ, на ОІД, де циркулює інформація.

У спеціальній частині складено акт обстеження на об’єкті інформаційної діяльності, розглянуто загальні відомості про підприємство, його організаційну структуру, аналіз середовища функціонування об’єкта інформаційної діяльності, класифікована інформація, що обробляється у інформаційно-телекомунікаційній системі та наведено характеристику компонентів системи. Також розроблено моделі загроз та порушника безпеки інформації, проаналізовані ризики для інформації і сформовані основні положення політики безпеки інформації для комплексної системи захисту інформації.

В третьому розділі визначено економічну доцільність впровадження ПБ. Проведено розрахунки капітальних витрат, поточних витрат, оцінки величини збитку та загальний ефект від впровадження КСЗІ.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ПОКАЗНИК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ.

# РЕФЕРАТ

Пояснительная записка: с., рис., табл., прилож., источников.

Объект разработки: информационно-телекоммуникационная система ЧП «ТехноСервис».

Предмет: политика безопасности информации объекта информационной деятельности (ОИД).

Цель работы (проекта): разработать политику безопасности информации в ИТС ЧП «ТехноСервис».

Методы, используемые при разработке: наблюдение, сравнение, анализ, описание.

В первом разделе проведен анализ нормативно-правовой базы в сфере защиты информации и указана актуальность вопроса, поставлены задачи на внедрение системы защиты информации на объектах информационной деятельности, где циркулирует информация.

В специальной части составлен акт обследования на объекте информационной деятельности, рассмотрены общие сведения о предприятии, его организационная структура, анализ среды функционирования объекта информационной деятельности, классифицирована информация, обрабатываемая в информационно-телекоммуникационной системе, и приведено описание компонентов системы. Также разработаны модели угроз и нарушителя безопасности информации, проанализированы риски для информации и сформированы основные положения политики безопасности информации для комплексной системы защиты информации.

В третьем разделе определена экономическая целесообразность внедрения информационной политики безопасности. Проведены расчеты капитальных (фиксированных) расходов, текущих (эксплуатационных) расходов, оценки величины ущерба и общий эффект от внедрения системы информационной безопасности. Определены и проанализированы показатели экономической эффективности систему информационной защиты.

Практическое значение работы состоит в возможности ее использования для разработки КСЗИ на реальном ОИД. Результаты,полученные в дипломном проекте, могут быть использованы для разработки и внедрения КСЗИ на предприятии.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНОФРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, АКТ ОБСЛЕДОВАНИЯ, ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ, ПОКАЗАТЕЛЬ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ.

ABSTRACT

An Explanatory Note: p., fig., tables., add., sources.

The object of this study is information and telecommunication system of TechnoService PE.

The subject of this study: information security policy of information activity object.

The purpose of the study: developing the security policy in information and telecommunication system.

Methods that were used: observation, comparison, analysis, description.

The first part of the study contains an analysis of regulatory documentation in information security, set tasks for the implementation of the information security system for information activity object where the information circulates.

The main part of the study considers the general statements about the enterprise; organizational structure of the computer system are contained. Information activity object`s environment for the functioning; risk assessment; threat analysis of information security; main elements of the information security policy of information and telecommunication system are analyzed; the main regulations of the security policy are formulated.

In the economic part defines economic feasibility of implementing an information security policy. The calculations of capital (fixed) costs, current (operational) costs, a calculation of loss and the effect of the implementation of information security. Economic efficiency indicators of information system security are analyzed.

The analyses provide the opportunity to use the developed security policy for implementation in the information and telecommunication system of the enterprise.

INFORMATION SECURITY, INFORMATION ACTIVITY OBJECT, INFORMATION SECURITY POLICY, RISK ASSESSMENT, THREAT ANALYSIS, ECONOMIC FEASIBILITY, CAPITAL COSTS, OPERATING COSTS, ECONOMIC EFFICIENCY INDICATORS.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПП – приватне підприємство;

ЗУ – Закон України;

АС - автоматизована система;

ЕОТ - електронно-обчислювальна техніка;

ІБ - інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ТЗІ – технічні засоби інформації;

ПЕОМ – персональна електронно-обчислювальна машина;

СУІБ – система управління інформаційною безпекою;

МКД – магнітно-контактний датчик;

КВІ – канали витоку інформації.

# ВСТУП

Сучасні методи обробки, передачі та накопичення інформації сприяли появі загроз, пов'язаних з можливістю втрати, несанкціонованої модифікації та розкриття даних, які адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку ІТ.

Комп'ютерні інформаційні технології швидко розвиваються та вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності та доступності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.

Захищеність інформаційної системи від випадкового або навмисного втручання, що завдає шкоди власникам або користувачам інформації, залежить, в основному, від доступності (можливість за розумний час отримати необхідну інформаційну послугу); цілісності (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого зміни); конфіденційності (захист від несанкціонованого прочитання). Майже в кожній системі є така інформація , яка при розголошенні може завдати збитки власникам. Особливо актуальним стає питання інформаційної безпеки (ІБ) на підприємствах, організаціях, в яких обробляється інформація з обмеженим доступом.

Одним із систем захисту інформації є етап розробки політики безпеки (ПБ). Чим краще та точніше буде виконано аналіз ОІД, тим швидше та простіше буде адміністраторам безпеки розробити комплекс заходів, що складе основу ефективної ПБ інформації.

# РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧ

## 1.1 Стан питання

У сучасному світі розповсюдження комп'ютерних технологій і комп'ютерної техніки, повсюдне проникнення телекомунікаційних мереж майже в усі сфери життєдіяльності людини одночасно і полегшило (наприклад, створення та накопичення баз даних, автоматична обробка інформації, можливість миттєвого передання інформації на дуже великі відстані тощо), й ускладнило управління, виконання виробничих процесів та особисту комунікацію. Йдеться про необхідність створення безпечних умов використання віртуального простору, серед іншого захисту від небезпек, які виникають із боку злочинців. Аналізуючи матеріали [6], можна виділити неймовірну динаміку кіберзлочинності за 2009 – січень-серпень 2018 рр, що наведена нижче на рис. 1.1.

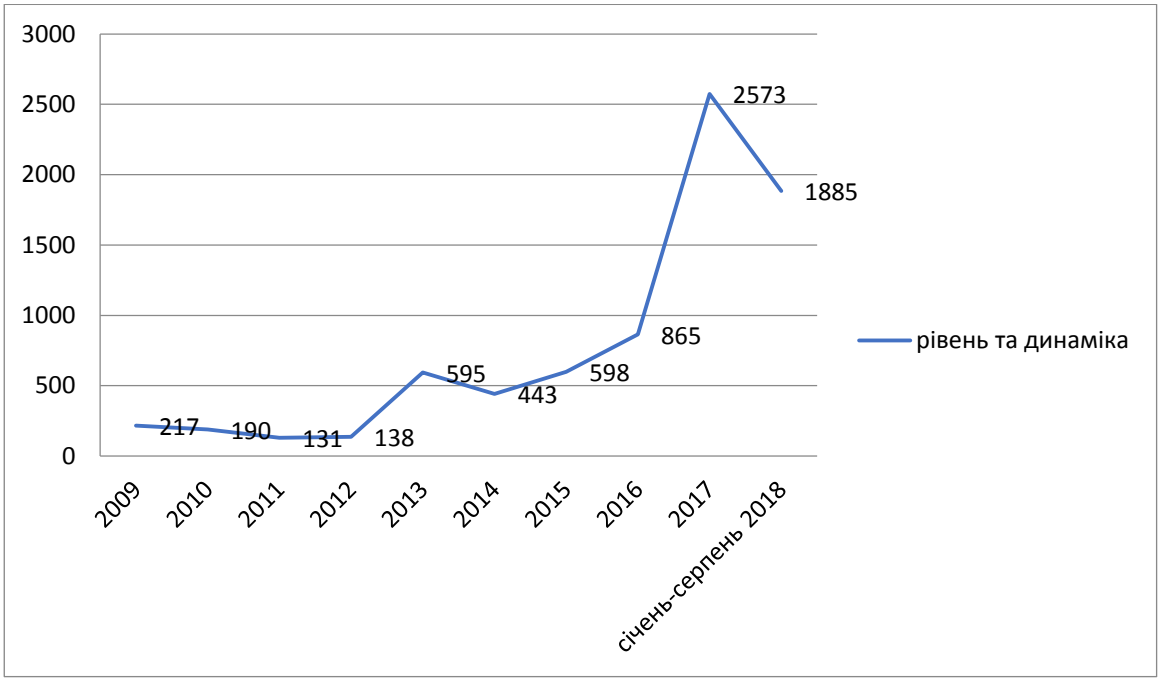



*Рис. 1.1 Графічне зображення рівня та динаміки кіберзлочинності в Україні за 2009 – серпень 2018 рр.*

Питома вага кіберзлочинів у загальній кількості зареєстрованих злочинів становить 0.05% від загальної кількості зареєстрованих злочинів у 2009 р., 0.04% - у 2010, 0.03% - у 2011, 0.03% - у 2012, 0.11% - у 2013, 0.08% - у 2014, 0.11% - у 2015, 0.15% - у 2016, 0.49% - у 2017 та 0.51% від злочинів, зареєстрованих за січень-серпень 2018 р. Для більшого розуміння ситуації нижче наведено

графічне зображення питомої ваги кіберзлочинів у загальній кількості зареєстрованих злочинів у 2009 – серпень 2018 рр.

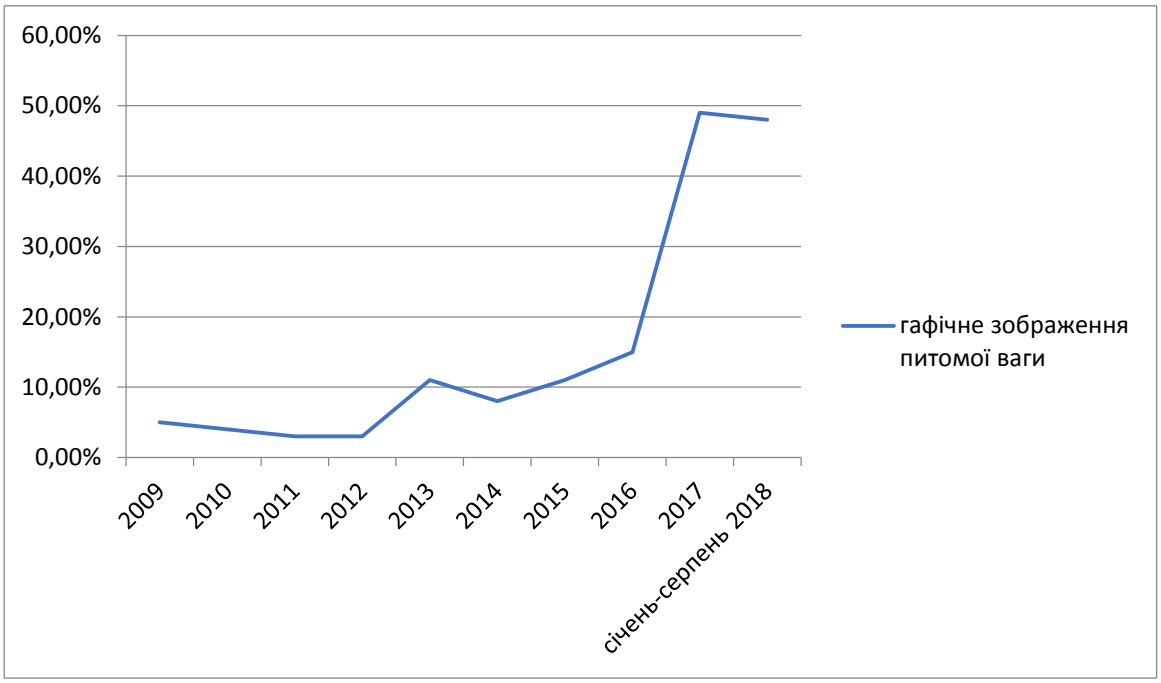



*Рис.1.2 Графічне зображення питомої ваги кіберзлочинів у загальній кількості зареєстрованих злочинів у 2009 – серпень 2018 рр.*

Статистичний аналіз поширення кіберзлочинів в Україні за данні роки виявив, що найвищий рівень злочинів було зареєстровано у 2017 році, це пов'язано з тим, що було впровадження мережі третього покоління (3G) операторами мобільного зв'язку,освоювання кібертехнологій як засобу злочинної діяльності, об'єктивне відставання технічної складової правоохоронної системи (активне реформування органів Національної поліції України, відсутність достатньої кількості фахівців та недостатнє фінансування) тощо.

В наш час жодна людина, організація або підприємство не реалізує свою діяльність без використання мережі Internet, тому проаналізувавши річний звіт з інформаційної безпеки Cisco 2018 [7] можна акцентувати увагу на способах проведення веб-атак за період жовтень 2014 – жовтень 2017 рр. Нижче наведена діаграма 1, де можна побачити, що протягом цього періоду зловмисники постійно впроваджували підозрілі виконавчі файли, в основному для доставки рекламного або шпигунського ПЗ. Такі типи потенційно небажаних програм можуть являти собою збільшення заражень шкідливого ПО і крадіжка

інформації про користувачів або компанії. Дані діаграми також показують, що обсяг шкідливого веб-контенту, що коливається в часі в міру того, як зловмисники запускають і завершують атаки і змінюють свої тактики, перешкоджаючи виявленню.

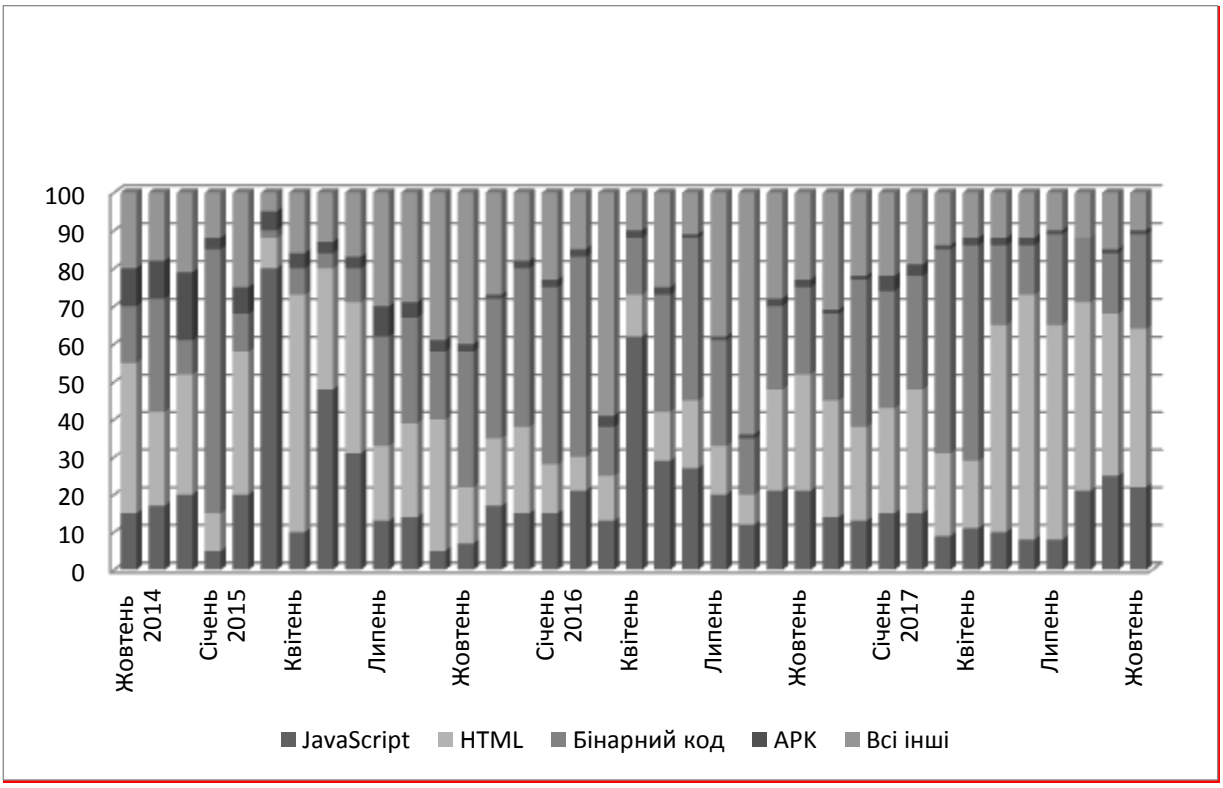



*Рис 1.3 Активність блоків на базі шкідливого ПЗ за типом контенту, жовтень 2014-жовтень 2017 рр.*

## 1.2 Аналіз нормативно-правової бази

Нормативно-правове забезпечення щодо захисту інформації - сукупність законів, нормативних актів та інших документів, що регламентують загальну організацію робіт, створення і функціонування конкретних систем захисту інформації.

Найважливішою складовою правового забезпечення у сфері захисту інформації є стандартизація, що має на меті:

- створення основних стандартів організаційно-методичного і термінологічного забезпечення системи захисту інформації;

- сталість вимог по захисту інформації в засобах обчислювальної техніки, в інформаційно-телекомунікаційних системах.

Тобто, нормативно-правове забезпечення регламентує та визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов’язані з інформаційною безпекою; етапи побудови КСЗІ. Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів, слід керуватися низкою нормативно-правових документів та актів.

Закони України, інші нормативно-правові акти України, державні стандарти, нормативно-правові акти і нормативні документи системи технічного захисту інформації в Україні формують та впроваджують єдиний в державі порядок забезпечення захисту інформації в ІТС.

Організаційно-розпорядчі, нормативні та інші документи, що використовуються у межах одної організації або ІТС, враховують усі особливості та умови обробки інформації в даній організації або ІТС.

В усіх нижчезазначених нормативних документах, а також у роботі в цілому, використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», або в інших нормативних документах з технічного захисту інформації, що вказані у розділі «Визначення».

В Україні є досить широка правова база щодо забезпечення безпеки інформації, але виділити можна деякі з них:

- Конституція України;
- Закон України (далі ЗУ) «Про інформацію»;

- Закон України «Про захист персональних даних»;

- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

- Закон України «Про електронний цифровий підпис»;

- Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373;

- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

Нижче наведена більш детальна інформація про виділені пункти.

Забезпечення безпеки інформації ґрунтується на системному підході та враховує вимоги та рекомендації стандартів:

- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010 – цей стандарт створений для визначення вимог для розроблення,впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

- ДСТУ ISO/IEC 27002:2015 - Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – цей міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження СУІБ на базі ISO/IEC 27001 або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановних документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища.

- ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) – цей стандарт надає настанови для управління ризиками інформаційної безпеки, а також підтримує основні концепції, визначені в ISO/IEC 27001, і розроблений для сприяння задовільному впровадженню інформаційної безпеки на основі підходу з управління ризиками.

Конституція України - основний закон України, який визначає права та обов´язки фізичних та юридичних осіб України та основний закон який забезпечує правові основи діяльності підприємства.

Закон України «Про інформацію» - висвітлює основні способи одержання, використання, поширення і збереження інформації. Він відображає право особистості на інформацію у всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відношень, регулює доступ до інформації і забезпечує її охорону, захищає особистість і товариство від помилкової інформації. У статтях закону визначаються категорії інформації і режим доступу до неї.

Закон України «Про електронний цифровий підпис» - цей закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису. Дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

Закон Україні «Про захист персональних даних» - цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» - регулює відносини у сфері захисту інформації в інформаційних,

телекомунікаційних та інформаційно-телекомунікаційних системах, визначає об`єкти та суб`єкти захисту в системі, встановлює відносини між власником системи, користувачами та володільцем інформації.

НД ТЗІ 1.1-002-99 визначає концепцію вирішення завдань захисту інформації в комп'ютерних системах та дає змогу вирішити питання з визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу, зі створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу та з оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

НД ТЗІ 1.1-005-07 визначає основи організації та етапи виконання робіт щодо створення комплексу на ОІД підприємства, яке має забезпечувати захист від витоку інформації з обмеженим доступом. Зміст цього документу можна використовувати під час обґрунтування, організації розроблення, впровадження заходів захисту ІзОД від загроз.

НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806, встановлює вимоги до змісту та структури нормативного документу, котрий регламентує діяльність служби захисту інформації в автоматизованій системі. Документ призначений для власників ІТС та користувачів, яких діяльність пов’язана з обробкою інформації в автоматизованих системах, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

В документі визначені функції служби захисту інформації з організації навчання персоналу з питань забезпечення захисту інформації; під час створення комплексної системи захисту інформації; під час експлуатації комплексної системи захисту інформації. Прописані права, обов`язки та відповідальність працівників служби захисту інформації.

НД ТЗІ 1.6-005-2013 визначає загальні вимоги з категоріювання, ознаку, за якою здійснюється категоріювання, а також порядок категоріювання об’єктів

інформаційної діяльності, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Положення є обов’язковим для підприємств незалежно від форми власності, на об’єктах яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці.

НД ТЗІ 3.1-001-07 визначає основні положення щодо проведення передпроектних робіт при створенні на об'єкті інформаційної діяльності підприємства ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом технічними каналами.

Цим НД встановлюються порядок та зміст проведення передпроектних робіт на ОІД, які вже функціонують або модернізуються, вимоги до оформлення акта обстеження на ОІД, а також вимоги до порядку розроблення та оформлення технічного завдання на створення комплексу ТЗІ.

НД ТЗІ 3.3-001-07 визначає порядок проведення робіт на об’єкті інформаційної діяльності підприємства на етапі розроблення та впровадження заходів із захисту від витоку інформації з обмеженим доступом технічними каналами під час створення комплексу ТЗІ.

НД ТЗІ 3.7-001-99 встановлює порядок розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі інформації з обмеженим доступом або інформації, захист якої гарантується державою. Положення цього документа розповсюджуються на державні органи, Збройні Сили, інші військові формування, МВС і органи місцевого самоврядування, а також підприємства, установи і організації всіх форм власності, які володіють, користуються і розпоряджаються інформацією, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники іншої інформації, положення цього документа застосовують на свій розсуд.

НД ТЗІ 3.7-003 -2005 визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах - порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Дія документу поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Його побудовано у вигляді керівництва, яке містить перелік робіт і посилання на діючі нормативні документи, у відповідності до яких ці роботи необхідно виконувати.

Нормативний документ призначений для суб'єктів інформаційних відносин, діяльність яких пов'язана з обробкою інформації, що підлягає захисту; розробників комплексних систем захисту інформації в ІТС; для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

ДСТУ 3396.1-96 установлює вимоги до порядку проведення робіт з технічного захисту інформації, що є обов`язковими для підприємств та установ усіх форм власності й підпорядкування.

Необхідність впровадження на реальному підприємстві комплексної системи захисту інформації продиктована вимогами стандартів України з управління інформаційною безпекою.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді

Під інформацією Закон України «Про інформацію» [1] розуміє сукупність документованих або привселюдно оголошуваних відомостей про події або явища, що відбуваються у суспільстві, державі й навколишньому середовищі.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [3] трактує інформацію як сукупність всіх даних і програм, використовуваних в автоматизованій системі, незалежно від способу їхнього подання.

Згідно закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.

Таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» захисту підлягає: відкрита інформація, яка є власністю держави і у визначенні Закону України «Про інформацію» належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (відкрита інформація). Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформаційний ресурс — сукупність документів у інформаційних системах.

Документом Закон України «Про інформацію» передбачено матеріальну форму одержання, зберігання, поширення й використання інформації шляхом фіксації її на магнітній, кіно-, відео-, фотоплівці або на іншому носії. Поняття «документа» важливо, оскільки документи є частиною інформаційних ресурсів і мають юридичну значимість.

Інформація з обмеженим доступом (яка підлягає захисту) може оброблятися, передаватися та зберігатися за допомогою обчислювальних ресурсів ІТС, а саме: серверів, робочих станцій, запам’ятовуючих пристроїв,

периферійних пристроїв (принтерів, накопичувачів на змінних магнітних носіях інформації), мережевого обладнання, системного та функціонального ПЗ, засобів, що забезпечують взаємодію об’єктів ІТС.

## 1.3 Постановка задачі

У нормативних документах зазначена необхідність впровадження системи захисту інформації, на об`єктах інформаційної діяльності, де циркулює інформація відкрита, що потребує захисту та інформація з обмеженим доступом. В іншому разі власник підприємства визначає потребу в КСЗІ. Під час обстеження ІТС потрібно розглядати як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

Потрібно проаналізувати й описати:

- загальну характеристику ОІД;
- загальну структурну схема і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо;
- умови функціонування ОІД, особливостей розташування його на місцевості тощо.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

## Висновки до розділу 1

В розділі 1 виконано оглядовий аналіз основної нормативно-правової бази, що стосується безпеки інформації, зазначено основні положення та проблематика захисту інформації в Україні.

Також наведені обґрунтування щодо потреби створення КСЗІ на підприємстві для запобігання НСД до важливої інформації. До етапів створення КСЗІ, що використані в роботі віднесені, відповідно до нормативної документації: обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує найбільш суттєві загрози.

# РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ПП «ТехноСервіс».

Об’єктом інформаційної діяльності (ОІД) є інформаційно-комунікаційних система підприємства «ТехноСервіс».

«ТехноСервіс» - приватне підприємство з передпродажної підготовки та продажу комп’ютерної техніки та периферії.

Форма власності: приватна власність.

В Україні розташувався поки що єдиний магазин. Приміщення, де розташований магазин – одноповерхове, розташоване на головній лінії, має площу 65 м2 . Щоденно магазин обслуговує близько 50-60 клієнтів.

Асортимент магазину «ТехноСервіс» має широку номенклатуру, а саме:

- планшети (планшетні комп’ютери);
- монітори;
- моноблоки;
- ноутбуки,ультрабуки;
- аксесуари для ноутбука,планшета та ін.;
- процесори;
- материнські плати;
- відеокарти;
- чіпи пам’яті ;
- вінчестери;
- корпуси;
- блоки живлення;
- стабілізатори живлення;
- звукові прилади;

- програмне забезпечення;
- обладнання для серверів;
- обладнання для відеоспостереження;
- інша периферія для комп’ютера.

## 2.2 Обґрунтування необхідності створення КСЗІ

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативно-правових документів розглянутих в Розділі 1 умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» об’єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов’язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об’єкті.

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об’єкта покладається на керівника установи-власника (розпорядника, користувача) об’єкта.

Об’єктами категоріювання є об’єкти інформаційної діяльності, в тому числі об’єкти ЕОТ.

Категоріювання здійснюється за ознакою:

– ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД;

– об’єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об’єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об’єктам може встановлюватися ІІІ категорія.

Об’єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об’єктів, який ведеться власником (розпорядником, користувачем) об’єктів інформаційної діяльності.

Простота і керованість інформаційної системи: принцип простоти і керованості інформаційної системи в цілому визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Забезпечення загальної підтримки заходів безпеки: принцип загальної підтримки заходів безпеки − носить нетехнічний характер. Рекомендується із самого

початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», ОІД, що розглядається встановлюється категорія IV (четверта) адже на об'єкті технічними засобами обробляється інформація з обмеженим доступом, що не становить державної таємниці.

На підставі проведеного аналізу власником інформації, яким виступає директор, прийняте рішення щодо створення КСЗІ та видано наказ «Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ПП «ТехноСервіс»» (Додаток В).

## 2.3 Обстеження на ОІД

Під час обстеження розглянуто середовище функціонування ІТС: обчислювана система, фізичне середовище, середовище користувачів та оброблювана інформація. Приводиться опис кожного середовища функціонування ІТС.

### 2.3.1 Обстеження обчислювальної системи

Обчислювальна система є локальною (ЛОМ) з виходом в Internet– з’єднуються пристрої, що розташовані в межах ОІД. Локальна мережа створена для забезпечення внутрішніх потреб підприємства.

ІТС ОІД представляє собою мережу типу «зірка», з окремо підключеним сервером та з використанням одного комутатору. Структурна схема представлена на рисунку 2.1, а також нижче в таблиці 1.1 та таблиці 1.2 наведені інвентаризаційні відомості елементів ІТС та додаткових технічних засобів.

ІТС являє собою комплекс, що обробляє різні категорії конфіденційності, а також має доступ до мережі Інтернет, який забезпечує ВАТ «Vega».

Обчислювальна система включає:

- чотири персональні електронно-обчислювальні машини (ПЕОМ), на яких встановлена операційна система Microsoft Windows 7 Максимальна, що об'єднані між собою витою парою 5-ої категорії для внутрішньої прокладки ;
- активне мережеве обладнання (Wi-Fi роутер (комутатор) на 10 портів);
- прикладне ПЗ (Microsoft Office, Total Commander, Google Chrome, WinRAR, Adobe Reader, Avast Pro, 1С підприємство 8.3, CCleaner, Winamp, Adobe Photoshop Elements 132.0.9.);
- периферійні пристрої вводу \ виводу даних HP LJ 1536, HP ScanJet 200.

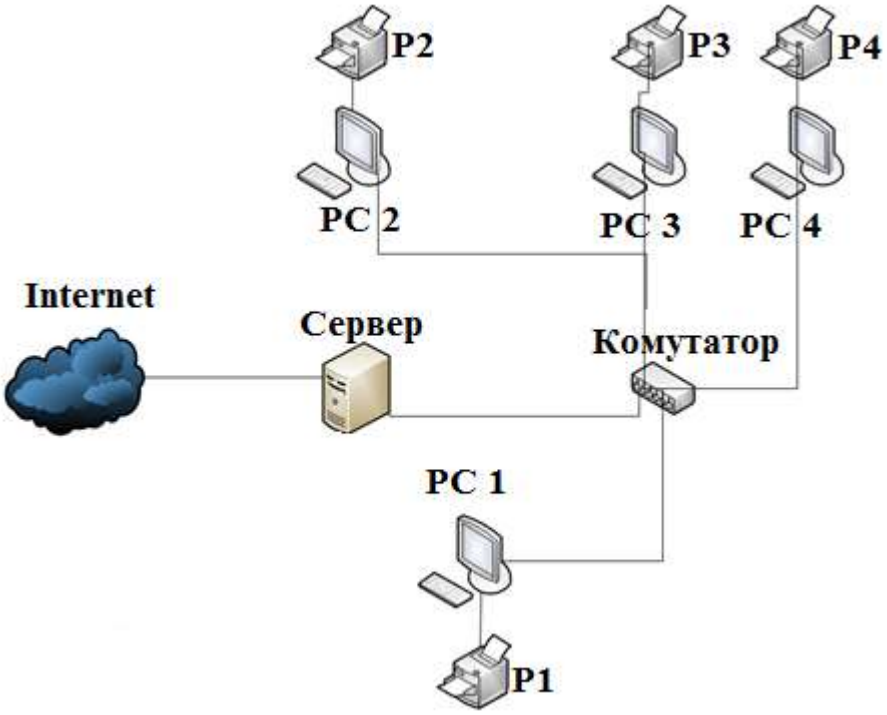



*Рис.2.1 Структурна схема «ТехноСервіс»*

*Таблиця 1.1 Інвентаризаційна відомість апаратного забезпечення ІТС ПП «ТехноСервіс»*

| № відповідно до плану | Назва | Характеристика | Ім'я в ІТС | Серійний номер | IP –адреса / MAC - адреса | Кількість | Відповідальна особа |
|---|---|---|---|---|---|---|---|
| 1 | Системний блок ASUS PN40-BB013M | Процесор Intel Celeron N4000/ ОЗУ 8GB/ Відеокарта Intel HD Graphics 600/ Материнська плата ASUS Mini PC PN40 | PC 1 | KS105UB | DHCP/ F1-7B-8F-EC-97-2E | 4 | Системний адміністратор |
| | | | PC 2 | VCX888 | DHCP/ 28-61-0D-99-D4-FF | | |
| | | | PC 3 | DE74L98 | DHCP/ 24-9C-02-DE-FE-BA | | |
| | | | PC 4 | YTR759E | DHCP/ 58-5A-B5-47-EA-D5 | | |
| | | | | | | | |

*Продовження таблиці 1.1 Інвентаризаційна відомість апаратного забезпечення ІТС ПП «ТехноСервіс»*

| № відповідно до плану | Назва | Характеристика | Ім'я в ІТС | Серійний номер | IP –адреса / MAC - адреса | Кількість | Відповідальна особа |
|---|---|---|---|---|---|---|---|
| 2 | Wi-Fi роутер (комутатор) D-Link DSR-250N | Інтерфейс : 1 x WAN Мбит/с 8 x LAN Мбит/с 1 порт USB 2.0 Консоль RJ-45/ Частота роботи: 2.4 ГГц / Скорость Wi-Fi: 150 Мбіт/с | R 1 | PI0D89S | DHCP/ FC-DC-9F-3F-A3-00 | 1 | Системний адміністратор |
| 3 | Сервер | Dell PowerEdge R720XD/ 2 x XEON | S 1 | IF7E2Q1 | 174.82.184.81 / F1-7B-8F-EC-97-2E | 1 | |
| | | | | | | | |

*Продовження таблиці 1.1 Інвентаризаційна відомість апаратного забезпечення ІТС ПП «ТехноСервіс»*

| № відповідно до плану | Назва | Характеристика | Ім'я в ІТС | Серійний номер | IP –адреса / MAC - адреса | Кількість | Відповідальна особа |
|---|---|---|---|---|---|---|---|
| 4 | Монітор | 21.5"LG 22M38A-B | PC 1-4 | SFE852G | - | 4 | 4 |
| 5 | Клавіатура | Sven Comfort 3535 | PC 1-4 | OL473PD<br>PIH976<br>FUOT54<br>OLPT96 | - | 4 | Системний адміністратор |
| 6 | Миша | ASUS ROG Sica USB Black | PC 1-4 | BI4588C<br>GTR74L<br>WER987<br>KOTGE5 | - | 4 | |
| 7 | Принтер | Canon PIXMA G1411 | PC 1-4 | AW963K<br>XQ96L5<br>ERT012 | - | 3 | |
| | | | | | | | |

*Продовження таблиці 1.1 Інвентаризаційна відомість апаратного забезпечення ІТС ПП «ТехноСервіс»*

| № відповідно до плану | Назва | Характеристика | Ім'я в ІТС | Серійний номер | IP –адреса / MAC - адреса | Кількість | Відповідальна особа |
|---|---|---|---|---|---|---|---|
| 8 | Камери відеоспостереження | Green Vision GV-047-GHD-G-COA20-20 1080P | Cam 1 | QT5C4S3 | 172.16.2.1/ 4E-17-2F-BF-DA-6C | 2 | Системний адміністратор |
| | | | Cam 2 | P8MH43Z | 172.16.2.2/ 4A-21-EE-05-22-7F | | |

*Таблиця 1.2 Інвентаризаційна відомість додаткових технічних засобів ПП «ТехноСервіс»*

| № | Назва | Модель | Серійний номер | Кількість | Відповідальний |
|---|---|---|---|---|---|
| 1 | Пасивні ІЧ датчики руху | DSC LC-100PI | YT85E90 | 6 | Системний адміністратор |
| | | | OI74UY1 | | |
| | | | IU967R0 | | |
| | | | EDR9FG | | |
| | | | RFVD6G | | |
| | | | SKIUY75 | | |
| 2 | Датчики на розбиття скла | PATROL-USR | 7S5F8T0 | 4 | |
| | | | 9H5J4Q6 | | |
| | | | 7K6G0F1 | | |
| | | | Q9W8E71 | | |
| 3 | Знищувач документів | Шредер Agent 007 S | AS4W5Y7 | 1 | |

На робочих станціях встановлені автоматизовані робочі місця (АРМ) з різним набором програмного забезпечення.

ІзОД в ІТС обробляється за допомогою наступних прикладних програм:

- АРМ «Керівник» (встановлене на РС 2 директора);
- АРМ «Адміністратор» (встановлене на РС 1 системного адміністратора);
- АРМ «Консультант» (встановлене на РС 3 та РС 4 консультантів-спеціалістів).

Детально програмне забезпечення, що встановлене в системі зазначено у таблиці 2.1.

*Таблиця 2.1 Інвентаризаційна відомість ПЗ ПП «ТехноСервіс»*

| № | Найменування | Комп'ютер на якому встановлено | Тип ліцензії | Ліцензійний номер |
|---|---|---|---|---|
| 1 | ОС Windows 7 Максимальна x64 (64-біт) | РС 1, РС 2, РС 3, РС 4 | Відсутня | - |
| 2 | Microsoft Office 2010 14.0.6023.1000 | | Відсутня | - |
| | | | | |

*Продовження таблиці 2.1 Інвентаризаційна відомість ПЗ ПП «ТехноСервіс»*

| № | Найменування | Комп'ютер на якому встановлено | Тип ліцензії | Ліцензійний номер |
|---|---|---|---|---|
| 3 | Google Chrome 74.0.03729.169 | PC 1, PC 2, PC 3, PC 4 | Відкрита | - |
| 4 | Total Commander 8.01 | | Відкрита | - |
| 5 | Avast Pro 19.5.4444 | | Відсутня | - |
| 6 | Adobe Reader 2019.008.20071 | | Відкрита | - |
| 7 | WinRAR 4.20 | | Відкрита | - |
| 8 | 1С підприємство 8.3 | PC 2, PC 3, PC 4 | Комерційна | C3-252DMN-HPR3F. |
| 9 | CCleaner 5.31.6105 | PC 1, PC 2 | Відкрита | - |
| 10 | Winamp 2.0 | PC 1, PC 2, PC 3, PC 4 | Відкрита | - |
| 11 | Adobe Photoshop Elements 132.0.9 | PC 2 | Відкрита | - |

2.3.2 Інформаційне середовище ОІД

В цьому пункті виконано аналіз інформаційного середовища та проведено класифікацію інформації відповідно до загальних вимог.

Вся інформація, що циркулює на ОІД вказана нижче в таблиці 2.2.

*Таблиця 2.2: Інформація,яка циркулює на ОІД та їх рівні конфіденційності, цілісності та доступності.*

| Інформація | Режим доступу | Правовий режим | Особи, що мають доступ | Рівень конфіденційності | Рівень цілісності | Рівень доступності |
|---|---|---|---|---|---|---|
| Облік внутрішніх документів (накази,службові записи, інструкції і т.д.) | З обмеженим доступом | Конфіденційна | Директор | К2 | Ц4 | Д4 |
| Інформація про надання послуг,тарифи,контактна інформація магазину | Відкрита як для працівників,так і для клієнтів | | Директор, консультанти-спеціалісти | К1 | Ц4 | Д3 |
| Інформація про робітників (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Конфіденційна | Директор, бухгалтер | К4 | Ц3 | Д3 |
| | | | | | | |

*Продовження таблиці 2.2: Інформація,яка циркулює на ОІД та їх рівні конфіденційності, цілісності та доступності.*

| Інформація | Режим доступу | Правовий режим | Особи, що мають доступ | Рівень конфіденцій-ності | Рівень цілісно-сті | Рівень досту-пності |
|---|---|---|---|---|---|---|
| Статутні документи підприємства (зберігається на сервері та в кабінеті у директора на паперовому носії) | Відкрита для працівників, клієнтів та перевіряючих | | Всі працівники | К1 | Ц4 | Д3 |
| Облік і реєстрація вхідних та вихідних документів організації (зберігається на сервері та в кабінеті у директора на паперовому носії) | З обмеженим доступом | Конфіденційна | Директор | К4 | Ц3 | Д5 |
| | | | | | | |

*Продовження таблиці 2.2: Інформація,яка циркулює на ОІД та їх рівні конфіденційності, цілісності та доступності.*

| Інформація | Режим доступу | Правовий режим | Особи, що мають доступ | Рівень конфіденційності | Рівень цілісності | Рівень доступності |
|---|---|---|---|---|---|---|
| Трудові договори робітників (зберігається на сервері та в кабінеті у директора на паперовому носії) | Відкрита для працівників | | Всі працівники | К4 | Ц4 | Д4 |
| Відомості про фінанси підприємства (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Директор,бухгалтер | К4 | Ц4 | Д5 |
| Відомості про постачальників (зберігається а сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Директор, консультант-спеціаліст, бухгалтер | К4 | Ц3 | Д4 |
| | | | | | | |

*Продовження таблиці 2.2: Інформація,яка циркулює на ОІД та їх рівні конфіденційності, цілісності та доступності.*

| **Інформація** | **Режим доступу** | **Правовий режим** | **Особи, що мають доступ** | **Рівень конфіденційності** | **Рівень цілісності** | **Рівень доступності** |
|---|---|---|---|---|---|---|
| Відомості про реалізацію продукції (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Директор,бухгалтер | К3 | Ц3 | Д3 |
| Зміст та характер договорів, контрактів, однією із сторін яких виступає підприємство (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Директор, консультант-спеціаліст | К2 | Ц4 | Д5 |
| | | | | | | |

*Продовження таблиці 2.2: Інформація,яка циркулює на ОІД та їх рівні конфіденційності, цілісності та доступності.*

| Інформація | Режим доступу | Правовий режим | Особи, що мають доступ | Рівень конфіденційності | Рівень цілісності | Рівень доступності |
|---|---|---|---|---|---|---|
| Відомості щодо обладнання приміщення підприємства охоронною сигналізацією та місце її встановлення (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Системний адміністратор,директор | К4 | Ц3 | Д5 |
| Відомості щодо наданої гарантії (зберігається на сервері та в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Системний адміністратор,директор, консультант-спеціаліст | К3 | Ц3 | Д4 |
| Копії товарних чеків (зберігається в кабінеті у директора паперовому носії) | З обмеженим доступом | Комерційна | Директор, консультант-спеціаліст | К2 | Ц3 | Д3 |

***Рівні конфіденційності:***

- К1– рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;
- К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
- К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;
- К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

***Рівні цілісності:***

- Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;
- Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
- Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;
- Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;
- Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

***Рівні доступності:***

- Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
- Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
- Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;
- Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;
- Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Основні інформаційні потоки:

*Облік внутрішніх документів* - завантажується на сервер,де працівники можуть ознайомитись, та одночасно друкується директором, щоб зберігати в спеціально відведеній папці.

*Інформація про надання послуг,тарифи,контактна інформація магазину* - використовується консультантами, щоб надати інформація клієнтам або ж клієнти можуть ознайомитись з цією інформацією, тому що вона знаходиться у вільному доступі.

*Інформація про робітників* - використовується директором в разі зміни працівників або у форс-мажорних ситуаціях (захворів, не прийшов на роботу та ін.).

*Статутні документи підприємства (правила діяльності організації)* - використовується клієнтами \ працівниками \ перевіряючими в разі потреби.

*Облік і реєстрація вхідних та вихідних документів організації (дані про продукцію,яка приїхала на склад, дані про продаж продукції)* - використовується консультантами, якщо клієнту потрібна консультація щодо замовлення тої чи іншої продукції, використовуються директором для контролю витрат та прибутку.

*Трудові договори робітників* – використовується \ змінюється директором в разі звільнення, прийняття або підвищення співробітника.

*Відомості про фінанси підприємства*-використовується бухгалтером при складанні звіту та директором для контролю фінансами.

*Відомості про постачальників* - використовується консультантом коли той робить замовлення продукції, використовується бухгалтером для оформлення кошторису та використовується директором для контролю та аналізу постачальників.

*Відомості про реалізацію продукції* - використовується бухгалтером при складанні звіту та директором для контролю продажів магазину.

*Зміст та характер договорів, контрактів, однією із сторін яких виступає підприємство* - використовується консультантом для надання інформації клієнту, якого цікавить з яким підприємством ми співпрацюємо (звісно якщо не йде мова про постачальників) та використовується директором при складанні \ підписанні цих договорів для пошуку вигідної співпраці.

*Відомості щодо обладнання приміщення підприємства охоронною сигналізацією та місце її встановлення* - використовується системним адміністратором для контролю за станом\працездатністю обладнання та використовується директором при закупівлі\оновленні того чи іншого обладнання.

*Відомості щодо наданої гарантії* - використовуються системним адміністратором для контролю за станом\працездатністю обладнання (обміном\поверненню\ремонту за діючою гарантією,якщо вона присутня), використовується консультантом для надання

гарантії на продукцію чи послуги магазину та використовується директором для контролю.

*Копії товарних чеків* - використовується консультантом для відновлення вже наданого товарного чеку (через втрату клієнта, звісно тільки після ідентифікації та підтвердження) та використовується директором для контролю за цим процесом.

*Загальний інформаційних потоків:*

1) облік внутрішніх та статутних документів;
2) облік інформації про надання послуг,тарифи,контактна інформація магазину;
3) облік інформації про робітників;
4) облік і реєстрація вхідних та вихідних документів організації;
5) облік трудових договорів робітників;
6) облік відомостей про фінанси підприємства та відомостей про постачальників;
7) облік відомостей про реалізацію продукції;
8) облік договорів, контрактів, однією із сторін яких виступає підприємство;
9) облік відомостей щодо обладнання приміщення підприємства охоронної сигналізації і місце її встановлення;
10) облік відомості щодо наданої гарантії;
11) облік копій товарних чеків.

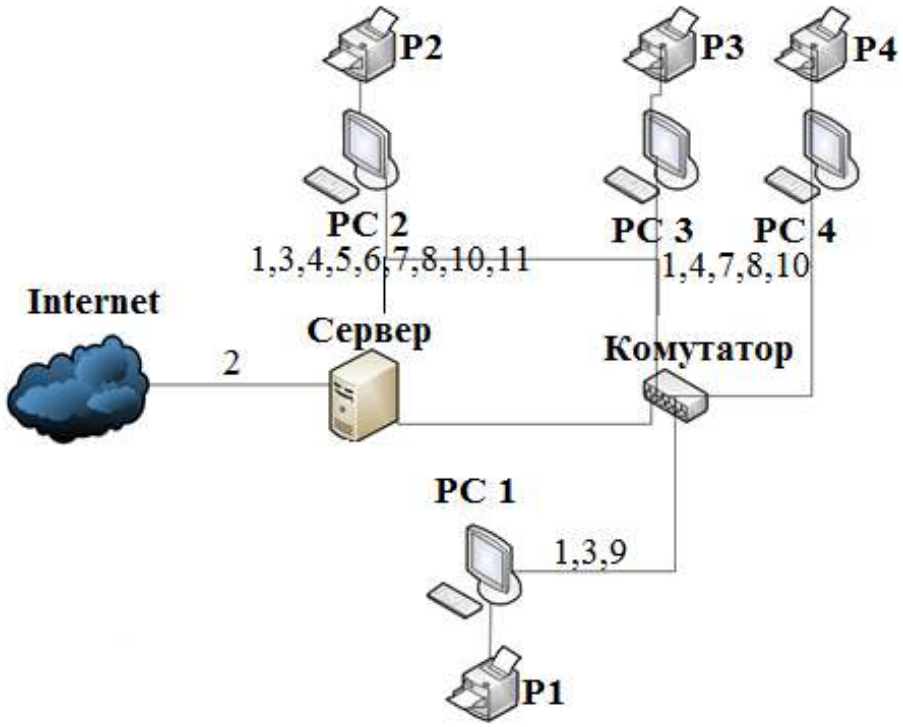



*Рис 2.2.: Схема інформаційних потоків на підприємстві*

Нижче, в табл.2.3, наведена матриця доступу до інформації, тобто що саме дозволено робити з довіреною інформацією (по списку):

- С – створення
- Ч – читання
- З – зберігання
- К – копіювання
- М – модифікація
- Д – друк
- В – видалення/знищення

*Таблиця 2.3: Матриця доступу до інформації*

| Користувачі | Інформація |
|---|---|
| Системний адміністратор | 1,4,6 - Ч,З,М,Д<br>2-Ч<br>11-Ч,К,М,Д,В |
| Консультанти | 1,2,4,8,10, 12,13 - Ч,С,З,В |
| Бухгалтер | 1-Ч<br>2-Ч,С,З,К,М,Д,В<br>3-Ч,С,З,Д,В<br>6-Ч,С,З,К,М,Д,В<br>9,10,22 - Ч,С,Д,М,З |

Доступ до ресурсів регламентується посадовими обов'язками та наказами директора, але явних заборон на використання ресурсів не виявлено.

2.3.3 Обстеження фізичного середовища

ОІД – «ТехноСервіс» є одноповерхова будівля.

Стіни будівлі, в якій знаходиться ОІД зроблені з вогнестійкої силікатної цегли (25х12х6,5 см). Фундамент – стрічковий, дах – покритий руберо1дом з

грубозернистим посипанням з лицьового боку і полімерною плівкою з наплавляємого боку полотна, територія навколо будівлі покрита асфальтом. Внутрішні та зовнішні стіни офісу – цегляні. Товщина зовнішніх стін – 380мм (3 шари цегли із цементом та внутрішньою штукатуркою), внутрішніх несучих стін – 250мм (3 шари цегли із цементом та штукатуркою), внутрішніх перегородок – 65мм (металоконструкція та гіпсокартон). Вікна – металопластикові, подвійні, 2100 х 1500мм. Вхідні двері – металопластиковідвустулкові з подвійним армованим склом – 2000мм шириною і висотою 2500мм. Замок - врізний зі сталі, закривається вбудованим циліндром під ключ з перфорацією. Міжкімнатні двері – металопластикові 90 х 2100 х 100 мм. Офіс має висоту 3м (від підлоги до стелі), стеля – натяжна, з металевим коробом по периметру стелі. Підлога на підприємстві – лінолеум.

2.3.4 Обстеження середовища користувачів

Штат працівників:

1. Директор

2. Системний адміністратор – 1 чол.

3. Консультант-спеціаліст – 2 чол.

4. Прибиральниця – 1 чол.

5.Бухгалтер – 1 чол.

Серед персоналу основними користувачами мережі є – системний адміністратор, директор та консультанти-спеціалісти. Бухгалтер працює на одному комп’ютері з директором. Нижче в таблиці наведені суб’єкти доступу до інформації.

*Таблиця 2.4 Суб'єкти доступу до інформації ПП «ТехноСервіс»*

| № | ФІО | Умовне позначення пристрою | Роль в інформаційній системі | Посада | Контактні дані |
|---|---|---|---|---|---|
| 1 | Грос Віктор Вікторович | PC 1 | адміністратор | Системний адміністратор | v.gros@gmail.com +380967280146 |
| 2 | Коваль Роман Петрович | PC 2 | користувач | Директор | r.koval@gmail.com +380734829542 |
| 3 | Петрушенко Ольга Василівна | PC 2 | користувач | Бухгалтер | petrushenko@gmail.com +380502475942 |
| 4 | Лисяк Марк Романович | PC 3 | користувач | Консультант-спеціаліст | m.lusyak@gmail.com +380730249632 |
| 5 | Литвін Марина Олексіївна | PC 4 | користувач | Консультант-спеціаліст | m.lutvin@gmail.com +380639173865 |

Основні посадові обов'язки працівників:

Системний адміністратор:

1) забезпечення роботи комп'ютерної техніки, комп'ютерної мережі і програмного забезпечення в організації;
2) підготовка і збереження резервних копій даних, їх періодична перевірка і знищення;

3) встановлення і конфігурування оновлень операційної системи, прикладного програмного забезпечення, нового програмного та апаратного забезпечення;
4) оновлення та підтримання інформаційної безпеки підприємства;
5) своєчасний звіт праці;
6) усунення неполадок у комп'ютерній системі магазину;
7) настройка кооперативного виходу в Інтернет;
8) підтримувати техніку в робочому стані;
9) настройка віддаленого доступу до мережі підприємства;
10) встановлення та налаштування Windows та інших програм;
11) встановлення та налаштування усіх периферійних пристроїв;
12) збір ПК;
13) підтримка працездатності мережі та серверу;
14) знищення комп'ютерних вірусів та шкідливих файлів;
15) відновлення інформації з жорстокого диску.

Бухгалтер

1) визначає, формулює, планує, здійснює і координує організацію бухгалтерського обліку господарсько-фінансової діяльності підприємства, здійснює контроль за ефективним використанням матеріальних, трудових і фінансових ресурсів;
2) складає баланс підприємства;
3) організовує та контролює складання розрахунків щодо використання прибутків, затрат на виробництво, платежів до бюджету, своєчасність і правильність складання звітності;
4) здійснює контроль за додержанням порядку оформлення первинних та бухгалтерських документів, розрахунків і платіжних зобов'язань, витрачанням фонду оплати праці, встановленням посадових окладів, за проведенням інвентаризацій основних засобів, нематеріальних активів, товарно-матеріальних

цінностей, коштів, документів, розрахунків, перевірок організації бухгалтерського обліку і звітності, документальних ревізій на підприємстві;

5) організує складання щомісячного бухгалтерського обліку, квартальних та річних бухгалтерських звітів (за результатами інвентаризації)

6) виявляє нестачу, незаконне витрачання коштів і товарно-матеріальних цінностей, порушення фінансового та господарського законодавства;

7) забезпечує на основі даних первинних документів і бухгалтерських записів своєчасне складання бухгалтерської та податкової звітності, подання її за встановленим порядком відповідним органам.

Консультант-спеціаліст

1) надання консультації клієнтам щодо товарів магазину;
2) надання консультацій щодо програмного забезпечення;
3) обслуговування клієнтів щодо встановлення ПЗ та усунення неполадок;
4) надання послуг з ремонту ПК та інших периферійних пристроїв;
5) своєчасний звіт своєї праці;
6) продаж товару магазину;
7) перевіряти робочий стан комп'ютерної техніки, у разі потреби проводити профілактичні дії.
8) організація електронного документообліку.

## 2.4 Аналіз та оцінка інформаційних ризиків

Аналіз ризиків інформаційної безпеки розроблений на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності підприємства.

Представлений аналіз включає в себе:

- модель порушника;
- модель загроз;

- ідентифікація наслідків реалізації загроз;

- оцінку ризиків та ймовірності їх появи.

### 2.4.1 Модель порушника

Порушником вважається особа, яка здійснює спробу несанкціонованого доступу до об’єктів захисту (ознайомлення, модифікація, знищення, зміна режимів використання чи функціонування тощо).

Якщо враховувати умови функціонування ІТС, то порушниками можуть бути в першу чергу персонал та користувачі АС, які напряму пов’язані із забезпеченням функціонування ІТС, а також з обробкою інформації, що підлягає захисту.

Категорії осіб, до якої може належати порушник:

- внутрішні порушники (авторизовані користувачі ІТС, яким надано право доступу до ІзОД);
- технічний персонал, що обслуговує будівлю та співробітники служби безпеки (особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІТС і потенційно можуть отримати доступ до ІзОД);
- зовнішні порушники (особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв’язку та можуть здійснити дії щодо порушення діючої в ІТС політики безпеки).

Метою порушника є отримання необхідної інформації, отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Всі зазначені особи мають можливість помилково або цілеспрямовано, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які можуть призвести до порушення конфіденційності, цілісності та

доступності інформації, яка обробляється в ІТС.

У колонці «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника (можливих збитків). Рівень загрози характеризується наступними категоріями:

1 - незначний,

2 - низький,

3 - середній,

4 - високий,

5 - неприпустимо високий.

*Таблиця 2.5 Категорії порушників*

| Позначення | Категорія | Потенційний рівень загрози |
|---|---|---|
| П1 | Внутрішні порушники | 5 |
| П2 | Технічний персонал, що обслуговує будівлю та співробітники служби безпеки | 2 |
| П3 | Зовнішні порушники | 4 |

*Таблиця 2.6 - Специфікація моделі порушника за місцем дії*

| Позначення | Характеристика місця дії порушника | Рівень загрози |
|---|---|---|
| Д1 | Усередині приміщення, але без доступу до технічних засобів ІТС | 1 |
| Д2 | З робочих місць користувачів та персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту | 5 |
| Д3 | Без доступу до приміщень, в тому числі з зовнішніх каналів зв’язку, з можливістю застосування технічних засобів здобуття інформації оптичними, | 2 |

*Таблиця 2.7 - Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз*

| Позначення | Характеристика можливостей порушника | Рівень загрози |
|---|---|---|
| З1 | Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС | 1 |
| З2 | Має можливість запуску програм, що реалізують функції обробки інформації | 3 |
| З3 | Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС. | 5 |

*Таблиця 2.8 - Специфікація моделі порушника за мотивами здійснення порушень*

| Позначення | Мотив порушення | Рівень загрози |
|---|---|---|
| М1 | Безвідповідальність (недбалість, ненавмисне порушення) | 3 |
| М2 | Корислива цілеспрямованість (зловмисне порушення) | 5 |

*Таблиця 2.9 - Специфікація моделі порушника за часом дії*

| Позначення | Характеристика можливостей порушника | Рівень |
|---|---|---|
| Ч1 | Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час) | 4 |
| Ч2 | Під час функціонування ІТС | 5 |
| Ч3 | Під час перерв у роботі для обслуговування та ремонту | 3 |

*Таблиця 2.10 - Профілі можливостей порушників*

| Позначення | Категорія | Характер дій порушника | | | | Рівень загроз |
|---|---|---|---|---|---|---|
| | | Мотив | Можливості | Час дії | Місце дії | |
| П1 | внутрішні порушники | М1, М2 | З2 | Ч1, Ч2, Ч3 | Д2 | 4 |
| П2 | технічний персонал, що обслуговує будівлю та співробітники служби безпеки | М2 | З1 | Ч3 | Д1, Д2 | 2 |
| П3 | зовнішні порушники | М2 | З1 | Ч2 | Д3 | 3 |

2.4.2 Модель загроз

Загрози потенційно можуть завдати шкоди інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам.

Оскільки неможливо одержати достатньо об’єктивні дані про ймовірність реалізації більшості з наведених загроз, ймовірність реалізації загроз визначено за методом, що описаний нижче, на основі аналізу статистичних даних.

Шкала оцінки загроз:

К1 – визначає ступінь доступності до об’єкта

1 – в іншій країні (для техногенних) / немає доступу до об’єкта (для антропогенних);

2 – в тій самій країні (для техногенних) / віддалений доступ до об’єкта (для антропогенних);

3 – поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних) / фізичний несанкціонований доступ до об’єкта, несанкціоноване проникнення в приміщення (для антропогенних);

4 – в тому ж приміщенні (для техногенних) / доступ у приміщення, де знаходиться об’єкт (для антропогенних);

5 – сам об’єкт (для техногенних) / фізичний дозволенний доступ до об’єкта (для антропогенних).

К2 – присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу

1 – виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей; техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником;

2 – виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози; ПЗ та техніка оновлюється не постійно;

3 – виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загрози; ПЗ та техніка вразливі для деяких атак;

4 – виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози; відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка;

5 – мета виконавця; виконавець є експертом у методах, що реалізують загрозу (наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське ПЗ, тощо.

К3 – фатальність наслідків

1 – ОІД нічого не втратить, або наслідки будуть позитивними;

2 – Наслідками можна знехтувати;

3 – Наслідки відчутні, але несуттєві;

4 – Наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу;

5 – Наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

К загальне для загроз розраховується за формулою:

$$\text{К загальне} = \frac{\text{К1}*\text{К2}*\text{К3}}{125}.$$

В таблиці не розглядаються загрози, що використовують технічні канали витоку інформації (перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричних перетворень інформаційних сигналів, оптичних КВІ).

*Таблиця 2.11 Результати аналізу загроз та вразливостей інформації в ІТС*

| № | Загрози | Вразливості, що призведуть до реалізації загроз | Джерело | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|---|---|
| 1 | Несанкціонований доступ до інформації через Wi-Fi | - нерегулярна зміна паролів на Wi-Fi. | Зовнішнє | 3 | 3 | 3 | 0,22 |
| 2 | Несанкціонований перехват інформації на паперових або електронних носіях | - неналежне зберігання документів та пристроїв з інформацією підприємства. | Внутрішнє | 3 | 5 | 4 | 0,48 |
| 3 | Проникнення в приміщення | - неефективна система охорони;<br>- недостатній контроль за приміщенням. | Зовнішнє | 3 | 3 | 5 | 0,36 |
| 4 | Здійснення атак на ОС | - відсутність або неефективність антивірусного ПЗ;<br>- наявність незахищеного з’єднання. | Внутрішнє, зовнішнє | 5 | 4 | 3 | 0,48 |
| | | - | | | | | |

*Продовження таблиці 2.11 Результати аналізу загроз та вразливостей інформації в ІТС*

| № | Загрози | Вразливості, що призведуть до реалізації загроз | Джерело | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|---|---|
| 5 | Соціальна інженерія (шантаж, підкуп тощо) з корисливою метою | - неправильний підбір персоналу. | Внутрішнє | 4 | 4 | 3 | 0,38 |
| 6 | Одержання та використання атрибутів доступу системи сторонніми особами внаслідок необережного поводження користувачів | - передавання паролів у відкритому вигляді;<br>- необізнаність персоналу з питань інформаційної безпеки. | Зовнішнє | 4 | 5 | 1 | 0,16 |
| 7 | Несанкціоноване копіювання інформації | - відсутність журналу подій. | Внутрішнє | 4 | 3 | 3 | 0,28 |
| | | | | | | | |

*Продовження таблиці 2.11 Результати аналізу загроз та вразливостей інформації в ІТС*

| № | Загрози | Вразливості, що призведуть до реалізації загроз | Джерело | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|---|---|
| 8 | Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях | - недосвідченість персоналу. | Внутрішнє | 4 | 2 | 3 | 0,19 |
| 9 | Випадкове зараження програмних засобів комп'ютерними вірусами | - недосвідченість персоналу;<br>- вільний доступ до мережі Internet;<br>- неякісне антивірусне ПЗ. | Внутрішнє | 5 | 2 | 4 | 0,32 |

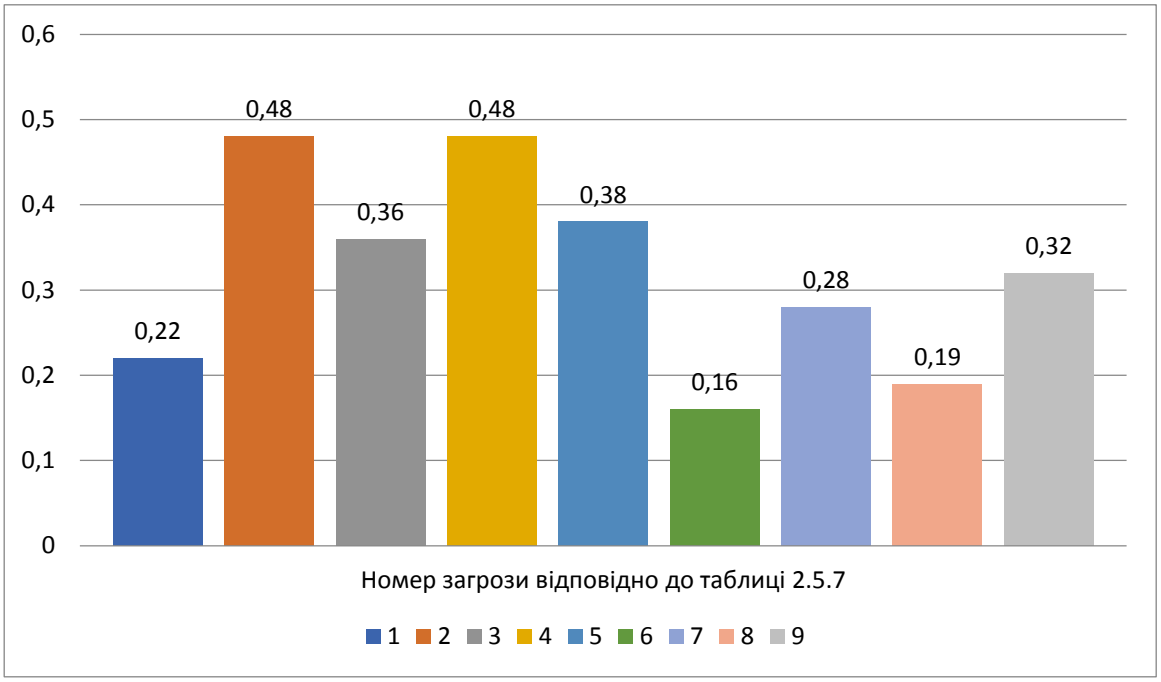



*Рис 2.3 Результати аналізу загроз та вразливостей інформації в ІТС*

Найбільш актуальними загрозами для ОІД вважаються:

- несанкціонований доступ до інформації через бездротову мережу (злам Wi-Fi);
- несанкціонований перехват інформації на паперових або електронних носіях;
- проникнення в приміщення;
- здійснення атак на ОС;
- соціальна інженерія (шантаж, підкуп тощо) з корисливою метою;
- несанкціоноване копіювання інформації;
- ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях.

Якщо ідентифіковані загрози будуть використовувати відповідні вразливості і призведуть до інциденту інформаційної безпеки, негативними наслідками для підприємства може стати повна або часткова втрата інформації, пошкодження або заміна інформації, скомпрометованість інформації. Ці інциденти вплинуть на ресурси підприємства. Таким чином, підприємство може отримати фінансові втрати.

Враховуючи характеристики існуючої ІТС та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99, обрано стандартний функціональний профіль захищеності для системи:

3.КЦ.1 = { КД-2, КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1 }

Перелік послуг, що входять в обраний профіль захищеності приведено посилаючись на НД ТЗІ 2.5-004-99 [8] зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

КД-2 Базова довірча конфіденційність, відноситься до Критерії конфіденційності - Довірча конфіденційність.

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

КВ-1 Мінімальна конфіденційність при обміні, відноситься до Критерії конфіденційності – Конфіденційність при обміні.

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

ЦД-1 Мінімальна довірча цілісність,відноситься до Критерії цілісності – Довірча цілісність.

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість.

ЦВ-1 Мінімальна цілісність при обміні,відноситься до Критерії цілісності – Цілісність при обміні

Ця послуга забезпечує мінімальний захист. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

НР-2 Захищений журнал, відноситься до Критерії спостереженості – Реєстрація

Ця послуга дозволяє контролювати небезпечні для КС дії.Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку.

НИ-2 Одиночна ідентифікація і автентифікація, відноситься до Критерії спостереженості – Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, який намагається одержати доступ до КС. Хоч поняття ідентифікація і автентифікація відрізняються, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем.

НК-1 Однонаправлений достовірний канал, відноситься до Критерії спостереженості – Достовірний канал

Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

НО-1 Виділення адміністратора, відноситься до Критерії спостереженості – Розподіл обов'язків

Дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НЦ-1 КЗЗ з контролем цілісності, відноситься до Критерії спостереженості – Цілісність комплексу засобів захисту

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна КС не може вважатися захищеною, якщо самі засоби захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

НВ-1 Автентифікація вузла,відноситься до Критерії спостереженості – Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

## 2.5 Розробка політики безпеки інформації

Спираючись на наявність ІзОД, яка обробляється в ІТС, фінансових на матеріальних ресурсів, обрано принцип розробки політики безпеки, при якому впровадження інформаційного захисту буде доцільним – досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС.

Усі заходи, що представлені в політиці безпеки, направлені на зниження ризиків реалізації загрози через вразливості ІТС, спираючись на існуючий аналіз ризиків (таблиця 2.11).

Першочергово необхідно ввести заходи для зниження ризиків по парі загроза/вразливість, що мають критичний рівень ризику 0,48. До цієї категорії відноситься несанкціонований перехват інформації на паперових або електронних носіях та здійснення атак на ОС.

Для зниження рівня ризику несанкціонованого перехвату інформації на паперових або електронних носіях розробляється політика безпеки «чистого столу», що включає організаційні методи та впровадження спеціального місця для зберігання паперових та електронних носіїв інформації. Також для зниження рівня ризику здійснення атак на ОС, розробляється політика антивірусного захисту, що включає організаційні та технічні методи та політика фільтрації використання мережі Інтернет користувачами системи, що також впливає на цей ризик.

# Політика «чистого столу»

1.Опис

Політика включає в себе інструкції для користувачів ІТС, що використовують на обробляються інформацію на паперових та електронних носіях.

2.Метою цієї політики є захист інформації на паперових та електронних носіях від несанкціонованого доступу.

3.Галузь застосування

Ця політика відноситься до всіх робітників підприємства.

4.Інструкція політики

Проаналізувавши стан робочих місць робітників підприємства, ввести регулярне прибирання столу, своєчасне складання документів в спеціально відведені місця.

Рекомендації для уникнення проблем з втратою або пошкодженням носіїв інформації:

- на початку роботи прибрати всі лишні предмети з робочого місця, протерти стіл;
- під час робочого дня не залишайте носії інформації без нагляду, навіть якщо збираєтесь на обідню перерву, то приберіть усі носії в спеціально відведене місце (в сейф), навіть якщо вони потім будуть потрібні для роботи;
- якщо тимчасово не має доступу до сейфу, то намагайтесь прибрати носії в недоступне місце (наприклад, в шафу робочого стола);
- в кінці робочого для завжди залишайте робоче місце в чистоті та всі документи відповідно приберіть у відведене місце.

5.Відповідальність

Відповідальність несе працівник, що порушив політику та може бути підданий стягненню.

6.Лист реєстрації змін.

7.Червень 2019  - політика впроваджена директором підприємства.

# Політика антивірусного захисту

## 1.Опис

Політика включає в себе інструкції для користувачів із застосуванням антивірусного ПЗ.

## 2.Метою цієї політики є захист системи від комп’ютерних вірусів.

## 3.Галузь застосування

Ця політика відноситься до всіх робітників підприємства, хто є користувачами системи.

## 4.Інструкція політики

Проаналізувавши антивірусне ПЗ, обрати серед доступних найефективніше. Антивірусне ПЗ має бути встановлене на всіх робочих станціях підприємства та постійно оновлюватись. Варто слідкувати за терміном дії ліцензії та продовжувати її заздалегідь.

Рекомендації для уникнення проблем з зараженням вірусів:

- на початку роботи з системою, переконайтесь, що антивірусне ПЗ увімкнено;
- не відкривайте сайти соціальних мереж або інші невідомі сайти;
- ніколи не відкривайте файли, прикріплені до електронного листа від невідомого або ненадійного джерела. Видаляйте одразу такі листі, навіть очищайте кошики;
- завжди при підключенні невідомого носія інформації скануйте його на наявність вірусів;
- не встановлюйте додаткове ПЗ з невідомого носія інформації шляхом відключення антивірусного ПЗ;

## 5.Відповідальність

Відповідальність несе користувач, що порушив політику та може бути підданий стягненню.

6.Лист реєстрації змін

7. Червень 2019 – політика впроваджена директором підприємства.

# Політика контролю використання мережі Інтернет користувачами системи

1.Опис

Контроль за використанням мережі Інтернет користувачами системи проводиться для зменшення інцидентів зараження системи вірусами.

2.Метою цієї політики є часткове обмеження доступу до мережі Інтернет.

3.Галузь застосування

Ця політика застосовується до всіх користувачів та робочих станціях, що підключені до мережі Інтернет.

4.Інструкція політики

Системний адміністратор має здійснювати контроль за використанням мережі Інтернет на всіх комп'ютерах, що є складовими системи. Для цього повинен вестись журнал, який фіксує дані: IP-адреса джерела, дату, час та місце. Та при можливості фіксувати ідентифікатор користувача. Записи про використання Інтернету мають зберігатися протягом 180 діб.

Необхідно проводити блокування доступу до Інтернет-сайтів, які вважаються ненадійними, до них відносяться сайти: з азартними іграми, сайти, що містять інформацію про зламування, соціальні мережі, чати та миттєві повідомлення, сайти, що містять порнографію та насильство. Перелік цих сайтів повинен переглядатися, змінюватися та доповнюватися.

5.Відповідальність

Відповідальність несе системний адміністратор та користувач, що порушив політику та може бути підданий стягненню.

6. Лист реєстрації змін.

7. Червень 2019 – політика впроваджена директором підприємства.

2.6 Аналіз інформаційних ризиків після впровадження політики безпеки

Повторний аналіз розробляється відповідно до методик та шкал, зазначених в таблицях розділу 2.4 Аналіз та оцінка інформаційних ризиків.

Метою цього аналізу є перевірка ефективності впровадження політик інформаційної безпеки.

В таблиці 2.12 – Рівень ризику після впровадження політики безпеки зазначені пари загроза/вразливість, що піддаються повторному аналізу, результати якого представлені на діаграмі 2.2.

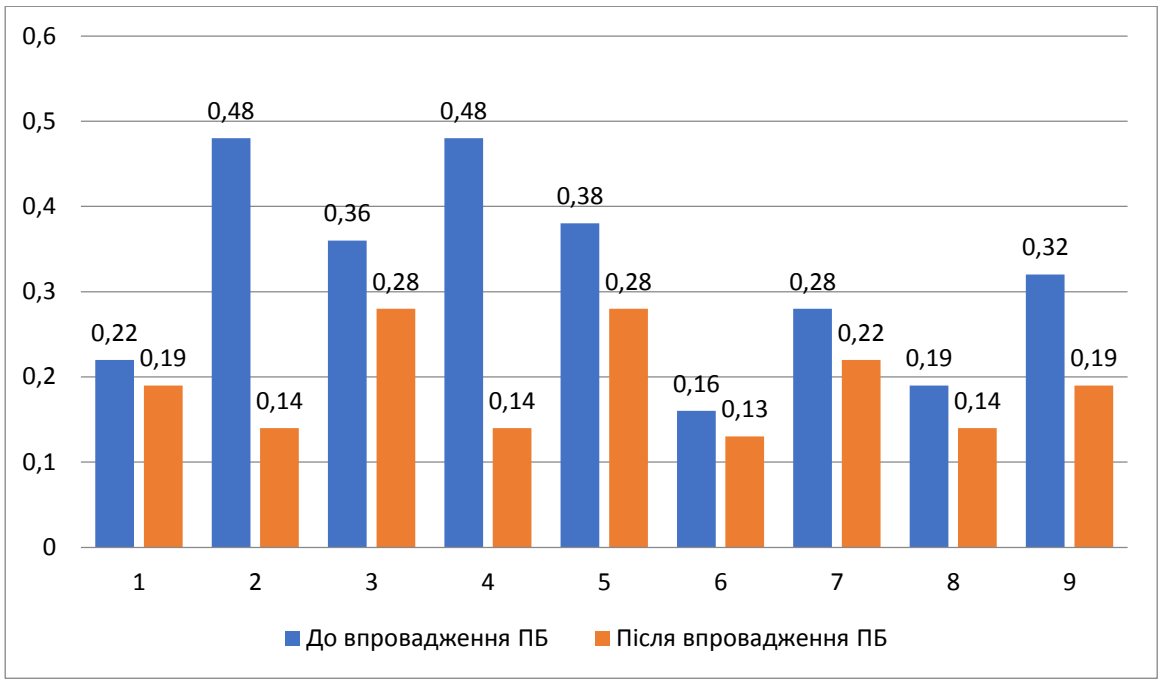



*Рис 2.4. Рівень ризику після впровадження політики безпеки*

Аналіз ризиків після впровадження розроблених інформаційних політик безпеки вказує на їх ефективність. Адже, рівень ризику, що розрахований за кожною парою загроза/вразливість, став меншим.

*Таблиця 2.12 Рівень ризику після впровадження політики безпеки*

| № | Загроза/вразливість | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|
| 1 | Несанкціонований доступ до інформації через бездротову мережу (злам Wi-Fi)/ нерегулярна зміна паролів на Wi-Fi | 4 | 3 | 2 | 0,19 |
| 2 | Несанкціонований перехват інформації на паперових або електронних носіях/ неналежне зберігання документів та пристроїв з інформацією підприємства | 3 | 3 | 2 | 0,14 |
| 3 | Проникнення в приміщення/ неефективна система охорони, недостатній контроль за приміщенням | 3 | 3 | 4 | 0,28 |
| | | | | | |

*Продовження таблиці 2.12 Рівень ризику після впровадження політики безпеки*

| № | Загроза/вразливість | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|
| 4 | Здійснення атак на ОС/ відсутність або неефективність антивірусного ПЗ, наявність незахищеного з'єднання | 3 | 2 | 3 | 0,14 |
| 5 | Соціальна інженерія (шантаж, підкуп тощо) з корисливою метою/ неправильний підбір персоналу | 4 | 3 | 3 | 0,28 |
| 6 | Одержання та використання атрибутів доступу системи сторонніми особами внаслідок необережного поводження користувачів/ передавання паролів у відкритому вигляді, необізнаність персоналу з питань інформаційної безпеки | 4 | 4 | 1 | 0,13 |
| | | | | | |

*Продовження таблиці 2.12 Рівень ризику після впровадження політики безпеки*

| № | Загроза/вразливість | К1 | К2 | К3 | $К_{загальне}$ |
|---|---|---|---|---|---|
| 7 | Несанкціоноване копіювання інформації/ відсутність журналу подій | 3 | 3 | 3 | 0,22 |
| 8 | Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях/ недосвідченість персоналу | 3 | 2 | 3 | 0,14 |
| 9 | Випадкове зараження програмних засобів комп'ютерними вірусами/ недосвідченість персоналу, вільний доступ до мережі Internet, неякісне антивірусне ПЗ | 4 | 2 | 3 | 0,19 |

## Висновки до розділу 2

У другому розділі було виконано обстеження ОІД, а саме розглянуто обчислювальну систему, інформаційне середовище, фізичне середовище та середовище користувачів. Проаналізовано та оцінено ризики інформаційної безпеки і виділено найбільш значущі загрози.

Згідно з проведеним аналізом, запропоновані до впровадження політики інформаційної безпеки в сфері інформаційного захисту від несанкціонованого доступу для забезпечення ефективної роботи всіх складових системи.

Аналіз ризиків запропонованих політик безпеки вказує на зниження рівня ризиків на систему через виявлені ризики.

# РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

## 3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою даного розділу є визначення витрат на впровадження політики безпеки інформаційно-комунікаційної системи ПП «ТехноСервіс».

Для визначення витрат проведено наступні розрахунки:

- капітальних витрат, що потребує політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика безпеки передбачає необхідність витрат на реалізацію. До заходів, що потребують витрат відноситься:

- впровадження правила «чистого столу»;
- оновлення ліцензій антивірусного ПЗ;
- навчання персоналу з питань інформаційної безпеки;
- витрати на керування доступом до мережі Інтернет.

## 3.2 Розрахунки витрат на впровадження політики безпеки

Розрахунок витрат на розробку політику безпеки підприємства

Тривалість створення політики безпеки визначається за формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{взз} + t_{озб} + t_{овр} + t_{д}, \text{годин} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{взз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

$t$ = 7+9+11+6+10+12+5 = 60 (год.)

Середня заробітна плата спеціаліста з питань захисту інформації з нарахуванням податків на даному підприємстві складає:

$$З_{зпг} = 70 \text{ грн/год}$$

Отже, витрати заробітна плата спеціаліста з питань захисту інформації за весь період розробки політики безпеки становить:

$$З_{зп} = t * З_{зпг} = 60 * 70 = 4200, \text{грн.} \qquad (3.2)$$

Витрати на розробку політики безпеки інформації розраховуються за формулою:

$$K_{рп} = З_{зп} + З_{мч}. \qquad (3.3)$$

А вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot C_{мч}, \text{ грн.} \qquad (3.4)$$

де $t$ – трудомісткість розробки політики безпеки інформації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}}, \text{ грн,} \qquad (3.5)$$

де $P$ – встановлена потужність ПК, кВт;

$C_{е}$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_{а}$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Оскільки на даному підприємстві встановлена потужність *P=0,6*, а тариф на електричну енергію становить 1.90 грн/кВт·година то:

$$С_{мч} = 1{,}90 * 0{,}6 * 4 + \frac{36000*0{,}8}{7680} + \frac{6000*0{,}8}{7680} = 8{,}91 \text{ грн.}$$

Отже, вартість машинного часу для розробки політики безпеки інформації на ПК становить:

$$З_{мч} = 60 * 8{,}91 = 534{,}6 \text{ грн.}$$

Тому, витрати на розробку політики безпеки інформації становлять:

$$К_{рп} = 4200 + 534{,}6 = 4734{,}6 \text{ грн.}$$

Визначена таким чином вартість розробки політики безпеки $К_{рп}$ є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пр} + К_{аз} + К_{навч} + К_{н}\,, \qquad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового ПЗ, тис. грн.;

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн.;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн..

Оскільки, підприємство не закуповує апаратне забезпечення для забезпечення

інформаційної безпеки, то $К_{аз}$ та $К_{н}$ не враховуються, а також враховуючі те, що розробка проекту інформаційної безпеки входить у вартість розробки політики безпеки, тому $К_{пр}$ не враховується.

Оскільки 1 ліцензійне оновлення коштує 1500 грн, то для 4 ПК $К_{зпз}=4*1500=6000$ грн.

Отже, $К =6000+4734,6 = 10734,6$ грн.

Розрахунок поточних (експлуатаційних) витрат

Для даного підприємства розрахунок експлуатаційних витрат складається з:

- навчання системного адміністратора;
- витрати на розмежування доступу до системи;
- витрати на керування системою інформаційної безпеки.

Розрахунок експлуатаційних витрат за рік за формулою 3.7:

$$С = Со + Спрд + Сз + Се + Стос \text{ грн.}, \qquad (3.7)$$

де Со – витрати на навчання системного адміністратора, Спрд – витрати на розмежування доступу до системи підприємства, Сз – додаткова заробітна плата системного адміністратора за проведення перевірки знань та навичок персоналу щодо правил регламентованих ПБ та додаткову відповідальність за виконання деяких розділів ПБ інформації, Се – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, Стос - витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки.

Розмір додаткової заробітної плати системного адміністратора складає 250 грн/міс., тобто річна додаткова заробітна плата складає 3 000 грн. Отже,

Сз = 3 000 грн.Оскільки навчання системного адміністратора проводиться 2 рази на рік, а вартість 1 навчання складає 500 грн, то витрати на навчання системного адміністратора складають 1000 грн. на рік, отже, Со = 1 000 грн.

Зарплатня нараховується за тарифом 70 грн/год. Робоча станція та монітор витрачають 0,6 кВт. Тариф на електроенергію становить 1,9 грн за 1 кВт/год. Впровадження ПРД займає 2 год раз на півроку.

Спрд = 2*2(0,6*1,9*70*0,22+70) =350,22 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е , \text{ грн,} \qquad (3.8)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

Fр – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

Це - тариф на електроенергію, грн/кВт·годин.

Оскільки на даному підприємстві встановлена потужність Р=0,6 кВт ,а Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 4 комп'ютера = 7680 год – річний фонд робочого часу системи інформаційної безпеки, то

$С_{ел}$ = 0,6*7680 * 1,9 = 8755,2 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

Сстос = К*0,02 = 10734,6*0,02 = 214,69 грн.

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

С = Со + Спрд + Сз + Се + Стос = 1000+350,22+3000+8755,2+214,69 = 13320,11 грн

Оцінка величини збиту

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки ($П_п$) .

Оскільки заробітна плата системного адміністратора разом з додатковою заробітною платою складає 9000 грн., то $З_с$ = 9000 грн.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \quad (3.9)$$

де Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Місячний фонд робочого часу складає 176 годин. Річний – 2 112 годин. Час простою внаслідок атаки 4 години:

$$П_п = (З_с / F) * t_a, \text{ грн.}, \quad (3.10)$$

де $З_с$ – загальна кількість витрат на заробітну плату співробітників за місяць, F – місячний фонд робочого часу, $t_a$ – час простою внаслідок атак.

Отже, $П_п$ =(9000/176)*4 = 204,5 грн.

Витрати на відновлення працездатності системи включають кілька складових:

$П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення системи, грн;

$П_{зч}$ – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ = 15 год:

$$П_{ви} = (З_с / F) * t_{ви}, \text{грн.}, \quad (3.11)$$

Отже, $П_{ви}$ =(9000/176)*15 = 767,04 грн.

Витрати на відновлення системи визначаються часом відновлення після атаки $t_в$ = 8 год. і розміром середньогодинної заробітної плати адміністратора:

$$П_{пв} = (З_{са}/F) * t_в, \text{ грн.}, \quad (3.12)$$

де $З_{са}$ – розмір середнього динної заробітної плати адміністратора, $t_в$ – час відновлення після атаки,F – місячний фонд робочого часу.

Отже, $П_{пв}$ =(4 500/176)*8 = 204,5 грн.

А вартість заміни частин системи в середньому становить $П_{зч}$= 2000 грн.

Звідси, витрати на відновлення працездатності системи:

$П_в = П_{ви} + П_{пв} + П_{зч}$= 767,04+204,5+2000=2971,54 грн.

Витрати від зниження працездатності атакованої системи:

$$V=O/F_r*(t_п + t_в + t_{ви}), \quad (3.13)$$

де tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, О – обсяг чистого прибутку підприємства за рік, $F_r$ - річний фонд часу роботи організації ($F_r$=2080 год.). Обсяг чистого прибутку підприємства за рік становить 180 000 грн., отже О= 180 000 грн., а $t_п$=4 год., $t_в$=8 год., $t_{ви}$=15 год

Отже, V=180 000/2080*(4+8+15) = 2336,53 грн.

Таким чином, упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

U = 204,5+2971,54+2336,53 = 5512,57 грн.

Оскільки кількість атак на рік складає 4 рази, а кількість комп’ютерів складає 4 шт., то загальний збиток від атаки на ІТС підприємства при реалізації загрози складає:

$$В = \sum_i \sum_п U \quad (3.14)$$

В = 4*4*5512,57 = 88201,12 грн.

Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження політики безпеки розраховується за формулою 3.13:

$$E = B \cdot R - C \text{ грн.}, \quad (3.15)$$

де, B – загальний збиток від атаки; R – очікувана ймовірность атаки на систему; C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Відповідно до аналізу інформаційних ризиків, реалізація загроз найймовірніша 1 раз на 3 місяці, тобто R= 0,25

Отже, E = 88201,12*0,25 – 13320,11 =8730,17 грн.

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

а) сукупна вартість володіння (ТСО);

б) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

в) термін окупності капітальних інвестицій То.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

ROSI = Е/К = 8730,17/10734,6 = 0,81

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ.

$T_o$ = 1/ ROSI = 1/0,81 = 1,2 років

Висновок до розділу 3

В розділі проаналізована доцільності впровадження політики безпеки інформації для інформаційно-комунікаційної системи ПП «ТехноСервіс». Визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Після всіх розрахунків вийшло, що капітальні витрати на впровадження інформаційної політики безпеки становлять 10 734,6 грн., експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 13320,11 грн.,а загальний збиток від атаки на ІТС підприємства складає 5512,57 грн.

Головне, що ефект від впровадження системи інформаційної безпеки становить 8730,17 грн., а термін окупності капітальних інвестицій складає 1,2 років.

Тому можна зробити висновок, що впровадження політики безпеки є доцільним.

# ВИСНОВКИ

Під час виконання дипломного проекту було:

- виконано оглядовий аналіз основної нормативно-правової бази;
- наведені обґрунтування щодо потреби створення КСЗІ;

До етапів створення КСЗІ, що використані в роботі віднесені, відповідно до нормативної документації: обґрунтування необхідності створення, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує найбільш суттєві загрози.

- виконано обстеження об’єкта інформаційної діяльності;
- визначено інформацію, що циркулює в інформаційно-комунікаційній системі ПП «ТехноСервіс» та яка підлягає захисту;
- проаналізовано загрози інформації та порушників;
- оцінено існуючий стан захищеності підприємства та обрано профіль захищеності;
- розроблено положення політики безпеки для інформаційної системи об’єкта інформаційної діяльності;

Аналіз ризиків запропонованих політик безпеки вказує на зниження рівня ризиків на систему через виявлені ризики.

- виконано економічне було розраховано витрати на впровадження політики безпеки.

Ґрунтуючись на отримані результати розрахунків, можна зробити висновок, що впровадження політики безпеки є доцільним.

На вимогу директора підприємства інформація, що використовувалась в ході роботи була змінена.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Закон України «Про інформацію»;
2. Закон України «Про захист персональних даних»;
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
4. Закон України « Про електронний цифровий підпис»;
5. Доктрина інформаційної безпеки України [Електронний ресурс]. –2014. – Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025 ;
6. Стаття Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні [Електронний ресурс] / Марина Олександрівна Кравцова. – 2018. – Режим доступу: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3848/Suchasnyi%20stan%20i%20napriamy%20protydii%20kiberzlochynnosti%20v%20Ukraini%20_Kravtsova_2018.pdf?sequence=1&isAllowed=y
7. Статистичні дані Cisco. [Електронний ресурс]. –2018. – Режим доступу: https://www.cisco.com/c/ru_ru/about/press/press-releases/2018/03-12.html
8. НД ТЗІ 2.5-004-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;
9. НД ТЗІ 1.1-002-99із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
10. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу;
11. НД ТЗІ 1.1-005-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення;

12. НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Типове положення про службу захисту інформації в АС;
13. НД ТЗІ 1.6-005-2013 - Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці
14. НД ТЗІ 2.5-005-99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;
15. НД ТЗІ 3.1-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи;
16. НД ТЗІ 3.3-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;
17. НД ТЗІ 3.7-001-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;
18. НД ТЗІ 3.7-003 -2005 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС;
19. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [Електронний ресурс]. – 2006. – Режим доступу: https://xn--80aagahqwyibe8an.com/kabineta-ministriv-postanovi/postanova-vid-bereznya-2006-373-pro152313.html
20. Проект Концепції інформаційної безпеки України[Електронний ресурс]. – 2015. – Режим доступу: http://mip.gov.ua/ru/documents/30.html

ДОДАТОК А. Перелік матеріалів на електронному носії

1. Дипломна робота – Таран Катерина, УБіт-15-1.docx
2. Презентація – Таран Катерина, УБіт-15-1.ppt

ДОДАТОК Б

**ПРИВАТНЕ ПІДПРИЄМСТВО «ТЕХНОСЕРВІС»**

НАКАЗ

_____ Дніпро № _____

Про визначення відповідального за забезпечення технічного захисту інформації та створення КСЗІ на ПП «ТехноСервіс»

З метою виконання вимог законів України «Про захист інформації в інформаційно – телекомунікаційних системах», «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно – телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, Положення про технічний захист інформації в Україні, затверджений від 27.09.1999 № 1229/99,

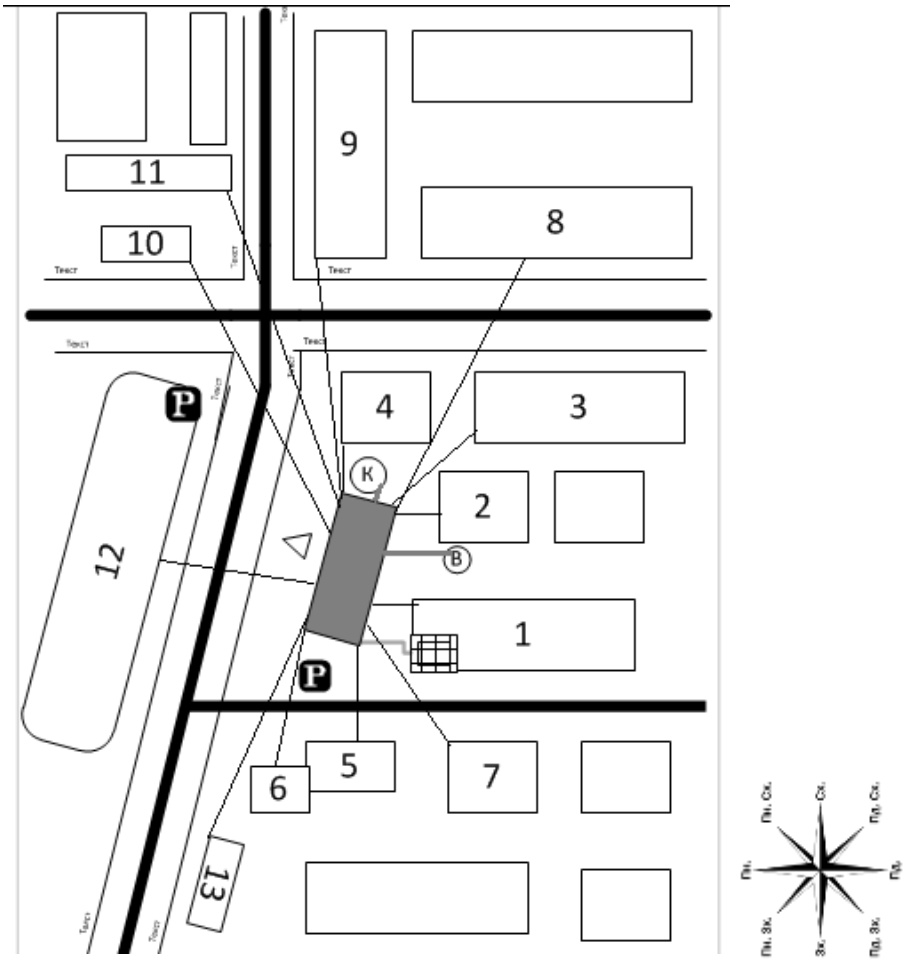
НАКАЗУЮ:

1. Відповідальність за забезпечення технічного захисту інформації в інформаційно – телекомунікаційній системі підприємства залишити за собою.
2. Створити комплексну систему захисту інформації (далі – КСЗІ) на підприємстві.
3. Затвердити:
   3.1. Політику безпеки локально – обчислювальної мережі підприємства.
   3.2. Перелік інформації, що підлягає технічному захисту на підприємстві.
4. Внести відповідні зміни до посадових інструкцій відповідних фахівців.
5. Провести категоріювання і обстеження складових ІТС підприємства.
6. Контроль за виконанням наказу покладаю на себе.

**Директор**

ДОДАТОК В. Ситуаційний план підприємства

*Рис.3 Ситуаційний план підприємства «ТехноСервіс»*




*Умовні позначення до рис. 3*

| | |
|---|---|
| | Пішохідна дорога |
| | Дорога |
| | Місце для паркування |
| | Вхід у будівлю |
| К | Люк міської системи каналізації |

| | |
|---|---|
| В | Люк міської системи водопостачання |
| | Трансформаторна підстанція |

ДОДАТОК Г. Генеральний план підприємства

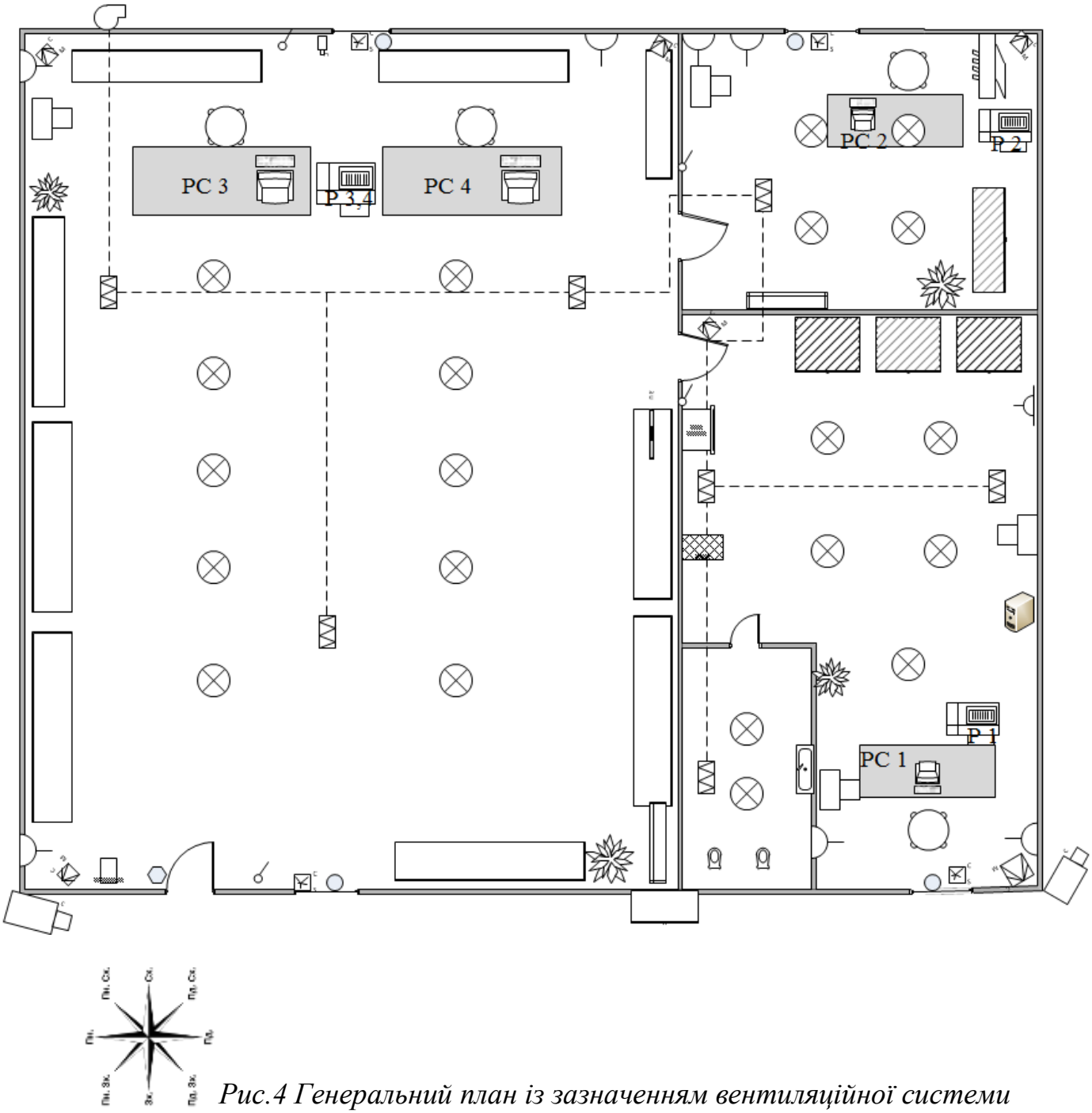



*Рис.4 Генеральний план із зазначенням вентиляційної системи підприємства*

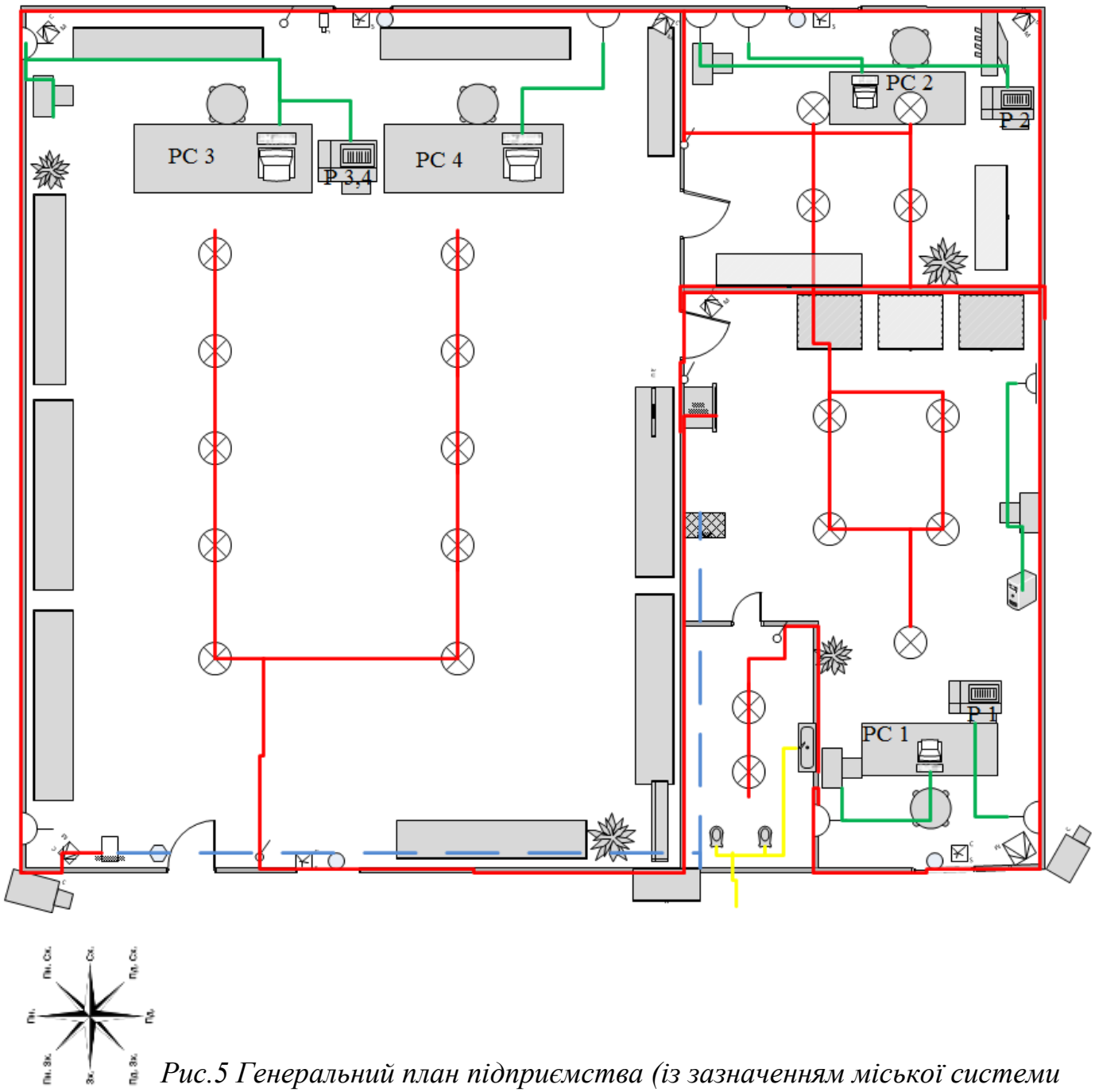
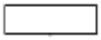
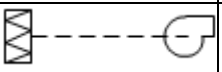
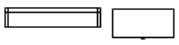



*Рис.5 Генеральний план підприємства (із зазначенням міської системи водопостачання, трас електрики, підключення техніки до мережі електроенергії, підключення ПКП до щитка сигналізації (частина 2))*

*Умовні позначення до рис.4 і рис.5*

| | |
|---|---|
|  | Wi-Fi роутер |
|  | Персональний комп’ютер |
|  | Принтер |
|  | Знищувач документів |
|  | Робоче місце |
|  | Вітрина |
|  | Шафа |
|  | Стілець |
|  | Вентиляційна система |
|  | Пасивний ІЧ датчик руху |
|  | Датчик розбиття скла |
|  | Електричний обігрівач |
|  | Камера відеоспостереження |
|  | Кондиціонер |
|  | Вимикач |

| | |
|---|---|
|  | Сервер |
|  | Розетка |
|  | Лампа |
|  | Лінії міської системи водопостачання |
|  | Лінії трас електрики |
|  | Лінії підключення техніки до мережі |
|  | Лінії підключення ПКП до щитка сигналізації |
|  | Щиток сигналізації |
|  | ПКП |
|  | Щитова (лічильник електроенергії) |
|  | МК датчик на відкриття вікна |
|  | МК датчик на вхідні двері |